S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
1.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.3. - Servers	75	Minimum 2*300 GB Hot Swap 15K SAS Self-encrypting drives	Every server OEM uses different technology for encrypting drives. Request to change below clause for wider OEM participation: "Minimum 2*300 GB Hot Swap 15K SAS drives with Self-encrypting drive or equivalent"	No Change
2.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.8. - SAN Storage	30	4. Minimum 4 Number of FC SAN Host Ports @16 Gbps or higher and Minimum 2 Number of IP SAN Host Ports @10Gbps or higher per controller.	It is clearly understood that the solution would require SAN Switch and SAN Connectivity is on FC SAN. Request to change this clause as "Minimum 4 Number of FC SAN Host Ports @16 Gbps or higher per controller."	No Change
3.	Corrigendum: Volume-II (Part-E)	—	S.No. 64	11	Capacity: The storage must support SAS, SSD and NL SAS disks simultaneously. For balanced performance, rebuild time & capacity, the storage should be provisioned with minimum 1300 TB of Usable capacity (In RAID 6, 8D+2P configuration) with maximum 8TB / 12 TB NL-SAS drives. Minimum two spare drives of proposed disk type to be provided for every Controller. 2 Drives of proposed capacity to be configured & kept at the site as cold spares.	Request to change this clause to " Capacity: The storage Solution must support SAS, SSD and NL SAS disks simultaneously. For balanced performance, rebuild time & capacity, the storage should be provisioned with minimum 1300 TB of Usable capacity (In RAID 6, 8D+2P configuration) with maximum 8TB / 12 TB NL-SAS drives. Minimum two spare drives of proposed disk type to be provided for every Controller. 2 Drives of proposed capacity to be configured & kept at the site as cold spares."	As per Corrigendum No. 4
4.	Volume-II (Part-E)	2.8. - SAN Storage		30	6. Cache: minimum 96GB DRAM cache across dual controller. Battery/Flash based cache protection for minimum 72 hours should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution.	Request to change the clause as "minimum 96 GB cache across all proposed controllers. Write Cache should be mirrored and complete cache protection through Battery/Flash based for minimum 72 hours in case of abrupt power shutdown. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution." for eider OEM participation.	No Change
5.	Volume-II (Part-E)	2.8. - SAN Storage		30	10. The capacity of the proposed configuration should be 100% scalable with the proposed disk configuration. No additional software/feature license or controller(s) should be required for further 100% capacity expansion. It should support SSD, NL-SAS and enterprise SAS Drives in the same enclosure for future expansions.	Request to change the clause as "The capacity of the proposed Solution configuration should be 100% scalable with the proposed disk configuration. No additional software/feature license should be required for further 100% capacity expansion. It should support SSD, NL-SAS and enterprise SAS Drives in the same enclosure for future expansions.	No Change
6.	Corrigendum: Volume-II (Part-E)	—	S.No. 69	12	Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & adding / upgrading controllers to the FC SAN & IP SAN fabric as well IP NAS network with all the proposed controllers managed from a One single GUI based management Interface. All requirements specified are minimum.	All OEM's have different storage architecture for Unified storage. Request you to modify the clause as "Proposed make of Unified All Flash storage Solution should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & adding / upgrading controllers to the FC SAN & IP SAN fabric as well IP NAS network with all the proposed controllers managed from a One single GUI based management Interface. All requirements specified are minimum. NAS Functionality can be provided through NAS Gateway if required by MSI/Bidder."	As per Corrigendum No. 4
7.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application	33	2. Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All	All OEM's have different storage architecture for Unified storage solution. Request to modify the clause as "Bidder is expected to provide Unified Storage solution should have block and file access (if solution requires) with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up . The storage solution must be dedicated appliance with specifically optimized OS to provide SAN and NAS functionalities. Proposed storage system must have minimum 2 controllers. The all proposed All Flash storage system should be categorized as All	Please refer Corrigendum No. 5

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
			Data)		Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs)."	
8.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	33	5. Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 32GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts	All OEM's have different storage architecture for Unified storage. Request to modify the clause as"Unified Storage controller nodes must be configured in minimum Dual-Controller configuration. Storage controller must have minimum 32GB on-board Protected cache per controller (Mirrored and Battery protected or Destage to Flash in case of abrupt power shutdown). The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts."	No Change
9.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	34	12. The Storage System should be able to protect the data against single point of failure with respect to controller, disks, cache, connectivity interfaces, fans and power supplies. Storage should support non-disruptive online microcode upgrades & support load balancing and failover without any limitation on SAN and NAS provisioned capacity.	To ensure online upgrades do not have impact on storage performance. Request to change clause as " Request to change clause as " The Storage System should be able to protect the data against single point of failure with respect to controller, disks, cache, connectivity interfaces, fans and power supplies. Storage should support non-disruptive online microcode upgrades which should not degrade the performance of the configured system & support load balancing and failover without any limitation on SAN and NAS provisioned capacity."	No Change
10.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.1. - 12-Port Layer 3 10G Switch (For Interconnecting)	18	18. Layer 3:- The Switch should support routing protocols such OSPF, BGPv4, IS-ISv4	Usually ISIS will never configured in LAN. Different OEMs uses different protocols in LAN for routing like OSPF. Kindly change the clause as Layer3 Features:- The Switch should support routing protocols such OSPF,BGPv4 IS-ISv4/OSPFv2/3 or equivalent.	No Change
11.	Volume-II (Part-E)	2.10. Unified storage with SAN Switch (75TB for Video and Application Data)	S.No 13	34	All the necessary software as specified in this RFP including capability to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc, single Command and GUI and Integrated Web Console for entire storage system for configuration for both file & block storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management.	Request to change the clause as "All the necessary software as specified in this RFP including capability to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc, Command and GUI and Integrated Web Console for storage solution for configuration for both file & block storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management."	No Change
12.	Volume-II (Part-E)	2.10. Unified storage with SAN Switch (75TB for Video and Application Data)	S.No 14	34	Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	Request to delete this clause as it is proprietary to one OEM.	No Change
13.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.1. - SAN Storage	72	Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up	All OEM's have different storage architecture for storage. Request to modify the clause as "Bidder is expected to provide Unified Storage solution should have block and file access (if solution requires) with host connectivity	Please refer Corrigendum No. 5

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
					and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	for FC/iSCSI/CIFS/ NFS. Storage should have the capability to scale up or scale-out . The unified storage solution must be dedicated appliance with specifically optimized OS to provide SAN and NAS functionalities. Proposed storage system must have minimum 2 controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs)."	
14.	Volume-II (Part-D)	4.2. Data Centre Hardware	4.2.1.1. SAN Storage	73	Storage should support protocol – FC, iSCSI, NFSv3, CIFS and SMB	Request to change this clause to "Storage should support protocol – FC/ iSCSI/ NFSv3/CIFS/SMB" Justification - MSI will not use all storage protocols for connectivity and since SAN switch has been asked only FC protocol will be primarily needed.	No Change
15.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	34	12. The Storage System should be able to protect the data against single point of failure with respect to controller, disks, cache, connectivity interfaces, fans and power supplies. Storage should support non-disruptive online microcode upgrades & support load balancing and failover without any limitation on SAN and NAS provisioned capacity.	To ensure online upgrades do not have impact on storage performance. Request to change clause as " The Storage System should be able to protect the data against single point of failure with respect to controller, disks, cache, connectivity interfaces, fans and power supplies. Storage should support non-disruptive online microcode upgrades which should not degrade the performance of the configured system & support load balancing and failover without any limitation on SAN and NAS provisioned capacity."	No Change
16.	Volume-II (Part-D)	4.2. Data Centre Hardware	4.2.1.1. SAN Storage	73	All the necessary software as specified in this RFP including capability to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc, single Command and GUI and Integrated Web Console for entire storage system for configuration for both file & block storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management.	All OEM's have different storage architecture for storage. Request to change the clause as "All the necessary software as specified in this RFP including capability to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc, Command and GUI and Integrated Web Console for storage solution for configuration for both file & block storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management."	No Change
17.	Volume-II (Part-D)	4.2. Data Centre Hardware	4.2.1.1. SAN Storage	73	Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	Request to delete this clause as it is proprietary to one OEM.	No Change
18.	Volume-II (Part-C)	NA				As per the Corrigendum, the specifications against Switching Fabric Architecture, Spine Switch, Leaf (Fibre) Switch stands deleted and out of RFP scope. Please confirm if our understanding is correct	Yes, the understanding is correct
19.	Corrigendum: Volume-II (Part-D)	__	S.No. 22	6	Router shall support IPSLA or equivalent and Y.1731 / 802.1ag for performance monitoring	For performance monitoring there are multiple ways to monitor the links like BFDs which is very effective way to monitore the links. Request you to kindly change the clause:- Performance:- Router shall support IPSLA or equivalent and Y.1731(OAM)/802.1ag or equivalent for performance monitoring	As per Corrigendum No. 4
20.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.2.2. - Core Router	80	Operating Environmental Requirements:- 0oC to 50oC operating temperature and 10 to 90%, non- condensing	Refer the response on a query of core router in Common RFP vol II - Part E - Common Specs where in the response on operating temperature and humidity is +/- 5%. Considering the same response and keeping the simitery in the specs,	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						Kindly change the clause as_ Operating Environmental Requirements:- 0oC to 45oC operating temperature and 15 to 90%, (+/- 5%) non- condensing	
21.	Volume-II (Part-D)	4.2.2. Network and Security	4.2.2.1. Internet Router	78	The proposed router shall support IEEE 1588v2 standard	There are multile standard protocols for time synchronization. Different OEM uses different standard protocol for the same like NTP. Request you to change the clause as:- The proposed router shall support IEEE 1588v2 standard/ NTP or equivalent	No Change
22.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.2.3. - Core Switch	80	General:- The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.	Redundant CPU is OEM specific. Different OEM uses different terminology to provide CPU redundancy in the same chassis. Our chassis would be populated with redundant management model which do have separate CPUs respectively to achieve the redundant factor. Request you to kindly change the same to :- The switch should have redundant CPUs/management module working in active-active or active-standby mode. CPU/management module in HA mode, fail over/change over should not disrupt/impact/degrade the functioning the switch.	No Change
23.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.2.3. - Core Switch	81	Performance:- Switch should support minimum 1000 VRF or equivalent instances	The ask VRF are very high and practically that much VRF will never get in use. That much number of VRFs generally used in telco environment and which is not the use case here. Request you to change the clause as :- Performance:- Switch should support minimum 250 VRF or equivalent instances	No Change
24.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.1. - 12-Port Layer 3 10G Switch (For Interconnecting)	18	Storage should support protocol – FC, iSCSI, NFSv3, CIFS and SMB	Request to change this clause to "Storage should support protocol – FC/ iSCSI/ NFSv3/CIFS/SMB" Justification - MSI will not use all storage protocols for connectivity and since SAN switch has been asked only FC protocol will be primarily needed.	No Change
25.	Corrigendum: Volume-II (Part-E)	__	S.No. 49	9	Router shall support IPSLA or equivalent and Y.1731 / 802.1ag for performance monitoring	For performance monitoring there are multiple ways to monitor the links like BFDs which is very effective way to monitore the links. Request you to kindly change the clause:- Performance:- Router shall support IPSLA or equivalent and Y.1731or equivalent for performance monitoring	As per Corrigendum No. 4
26.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.8. - SAN Storage	30	6. Cache: minimum 96GB DRAM cache across dual controller. Battery/Flash based cache protection for minimum 72 hours should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution.	As the capacity requirement is higher so request you to increase the cache from 96GB to 192GB, so that storage will be able to perform required throughput to cater the performance required in Smart cities. Also 72hours battery backup for the cache is not supported from many OEM, Hence request you to change the clause as below "Cache: minimum 192GB DRAM cache across dual controller. Battery/Flash based cache protection for minimum 72 hours/ destaging the data into the disks/drives should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution."	No Change
27.	Corrigendum: Volume-II (Part-E)	__	S.No. 69	12	Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system	"Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage	As per Corrigendum No. 4

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
					should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & adding / upgrading controllers to the FC SAN & IP SAN fabric as well IP NAS network with all the proposed controllers managed from a One single GUI based management Interface. All requirements specified are minimum.	can be scaled by adding capacity to the controllers & adding/upgrading controllers to the FC SAN & IP SAN fabric with all the controllers managed from a One single GUI based management Interface. All requirements specified are minimum."	
28.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	33	2. Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	75TB usable capacity having a scalability of 1.5x that is less than 120TB can be easily achievable having 2 controllers architecture. Storage OEMs provide different architectures to meet the customer requirement, like Scale up or Scale Out. Therefore requesting to change the requirement to Scale up or Scale out. Request you to accept the below change "Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up or scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs)."	Please refer Corrigendum No. 5
29.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	33	5. Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 32GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts	75TB usable capacity in unified solution requires higher cache to provide better performance, with the limitation in the cache storage having high cost and efficiency disks will not be able to provide performance. Hence request you to accept below change "Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 96GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts."	No Change
30.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	34	14. Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	Backup solution is already considered in the RFP which can take the backup of application & VMs, Also Data at rest Encryption should be enabled on hardware level which should be enabled with Internal or External Key management software, this provides storage systems to protect against unauthorized access to lost or stolen drives or system, Hence request you to consider the below change. "Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and Application & VM aware/consistent copies. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with hardware based (Controller / Disk based) data at rest encryption and key	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						management."	
31.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.1. - SAN Storage	72	Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & controllers to the FC SAN & IP SAN fabric as well IP NAS network with all the proposed controllers managed from a One single GUI based management Interface. All requirements specified are minimum.	250TB usable capacity having a scalability of 1.5x that is 375TB can be easily achievable having 2 controllers architecture. Storage OEMs provide different architectures to meet the customer requirement, like Upgrading Controllers or adding controllers . Therefore requesting to change the requirement to to add or upgrade controllers. Request you to accept the below change "Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & adding/upgrading controllers to the FC SAN & IP SAN fabric with all the controllers managed from a One single GUI based management Interface. All requirements specified are minimum."	Please refer Corrigendum No. 5
32.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.1. - SAN Storage	72	Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	250TB usable capacity having a scalability of 1.5x that is 375TB can be easily achievable having 2 controllers architecture. Storage OEMs provide different architectures to meet the customer requirement, like Scale up or Scale Out. Therefore requesting to change the requirement to Scale up or Scale out. Request you to accept the below change "Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up or scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs)."	Please refer Corrigendum No. 5
33.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.1. - SAN Storage	72	Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 32GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts.	250TB usable capacity in unified solution requires higher cache to provide better performance, with the limitation in the cache storage having high cost and efficiency disks will not be able to provide performance. Hence request you to accept below change "Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 96GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts."	No Change
34.	Volume-II (Part-D)	4 - Minimum Technical Specifications	4.2.1.1. - SAN Storage	73	Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest	Backup solution is already considered in the RFP which can take the backup of application & VMs, so assuming VM aware backup are mentioned for the snapshot or clone Also Data at rest Encryption should be enabled on hardware level which should be enabled with Internal or External Key management software, this provides storage systems to protect against unauthorized access to lost or stolen drives or system,	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
					encryption and key management.	Hence request you to consider the below change. "Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and Application & VM aware backup/consistent copies. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with hardware based (Controller / Disk based) data at rest encryption and key management."	
35.	Corrigendum: Volume-II (Part-A)	__	S.No. 15	5	X. Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines.	We understand that MSI has to propose storage encryption with a FIPS 140-2 KMIP V2.1 supported & compliant Key management server with capabilities of 25000 client connections and storage capacity of 25 lakhs and above encryption keys per dedicated appliance to achieve best of the encryption. As per the security guidelines, separating master keys from the application is a must and managed by a Key Management System.	As per Corrigendum No. 4
36.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.9 Security, Privacy and Compliance Requirement	56	The infrastructure elements including server, storage (including backup storage) and network of the Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from other tenants.	The infrastructure elements including server, storage (including backup storage) and network of the Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption through FIPS 140-2 Key management server to achieve Data Security & Data Confidentiality, FIPS 140-2 Key management server should have the capabilities like storage of 25 lakhs encryption keys and be logically separate from other tenants. All the storage element must to implement Data at Rest encryption and must keep in a separate FIPS 140-2 Level 2 Key Management System. It's never advised to keep keys within the storage or application.	No Change
37.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.9 Security, Privacy and Compliance Requirement	56	CSP should enable encryption of data both in rest and transit.	By this statement we understand that CSP has to provide "Data at Rest" & " Data in Transit" to achieve Data Security, Data Confidentiality, Data Privacy to adhere the India IT Act 2000, 2008 & amendment 2011. Hence it is mandatory to use a dedicated FIPS 140-2 Key Management appliance with capabilities of 25k client connections and storage capacity of 2.50Million and above encryption keys per dedicated appliance to achieve best of the encryption.	No Change
38.	Corrigendum: Volume-II (Part-A)	__	S.No. 29	8	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus, HIPS integration, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as Linux VMs, VM level encryption , secure boot, uninterrupted service delivery within and across datacentre at geographical distance (<100ms latency), distributed virtual switch, and storage virtualization technology.	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus, HIPS integration, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as Linux VMs, VM level encryption through dedicated FIPS Level 2 Key Management device, secure boot, uninterrupted service delivery within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology.	As per Corrigendum No. 4

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
39.	Corrigendum Volume-II (Part-B)	—	S.No. 03	2	The cameras shall support secure authentication mechanism for both ONVIF, and web based administrative access for the cameras.	The cameras shall support only secure PKI certificate-based authentication mechanism for both ONVIF, and web based administrative access for the cameras. The certificate authority as part of the PKI must be secured using FIPS 140-2 level 3 HSM with 15000 TPS & capabilities of unlimited client connection and unlimited partitions per appliance for scalability for self-signed certificates. HSM should support multiple authentication methonds on the same device like Smart Card, Key File & passwords, also HSM should provide field upgrade without changing the hardware.	As per Corrigendum No. 4
40.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	34	14. Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage must be configured with data at rest encryption and FIPS 140-2 KMIP Compliant Key Management Appliance.	No Change
41.	NA				Additional	OEM should provide the declaration on the Letter Head of the proposed solution / appliances, should not be announced End of Sales and Support for at least next 5 years from the Date of Opening of the bid.	No Change
42.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.10. - Unified storage with SAN Switch (75TB for Video and Application Data)	33	2. Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	Since Smart cities will Store lots of video data and application data so to handle video data effectively and for better performance requesting you to please rephrase to "Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs). The system should support File System Capacity of Min. 1PB The NAS System should support minimum 10Million Files per directory and expandable "	Please refer Corrigendum No. 5
43.	Volume-II (Part-E)	2.1. 12-Port Layer 3 10G Switch (For Interconnecting)	2.10. Unified storage with SAN Switch (75TB for Video and Application Data)	33	Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 32GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts.	please rephrase to Unified Storage controller nodes must be configured in Dual-Symmetric Active-Active configuration. Storage controller must have minimum 128GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts.	No Change
44.	Volume-II (Part-E)	2 - City Datacentre Active Infra	2.10. - Unified storage with	34	14. Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup.	Smart city will have Heterogeneous environment for data as well as performance/Scalability requirements for IT Infrastructure and make your investment future proof by providing option to connect old storage with new	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
		Equipment's	SAN Switch (75TB for Video and Application Data)		Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	storage. Hence requesting you to Please consider it and rephrase it to - "Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery. Storage should be configured with data at rest encryption and key management. The necessary hardware and software should be quoted for entire proposed capacity to connect any make & model external Storage for future expansion/scalability".	
45.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.8. - SAN Storage	30	6. Cache: minimum 96GB DRAM cache across dual controller. Battery/Flash based cache protection for minimum 72 hours should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution.	For better performance and scalability minimum cache should be 512GB across the controller, as per industry best practices for disk/controller ratio for optimum utilization and performance. top 5 storage manufacture also suggest to have this much minimum cache for enterprise class storage requirement (similar to this RFP) please rephrase it to - "Bidder is expected to provide SAN solution with minimum 512 GB DRAM Cache across the dual Symmetric Active-Active controllers with only write mirroring. Battery/Flash based cache protection for minimum 72 hours should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution."	No Change
46.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.6. - Network Intrusion Prevention System	26	2. The hardware should have minimum of 8x1G ports.	Requesting you to please rephrase it to "The hardware should have minimum of 4x1G/10G ports and 8 X 10G SFP+ ports; should support I/O slots for additional port requirements in future."	Please refer Corrigendum No. 5
47.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.6. - Network Intrusion Prevention System	27	8. The appliance should support a throughput of minimum 1 Gbps scalable to 4 Gbps within the same box and latency should be <50 ms for all kinds of real-world traffic/production performance in Active-Active or Active- Standby mode	Requesting you to please rephrase it to "The appliance should support a throughput of minimum 10 Gbps scalable to 30 Gbps within the same box and latency should be <50 ms for all kinds of real-world traffic/production performance in Active-Active or Active- Standby mode. The appliance should also support SSL inspection on the same appliance without relying on any third party solution and should support min throughput of 10 Gbps scalable to 15 Gbps with ssl inspection enabled."	No Change
48.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.6. - Network Intrusion Prevention System	27	9. The appliance should support minimum of 2,00,000 connections per second scalable upto 6,00,000 connections per second without changing the hardware	Requesting you to please rephrase it to "The appliance should support minimum of 4,00,000 connections per second scalable upto 6,00,000 connections per second without changing the hardware"	No Change
49.	Corrigendum: Volume-II (Part-A)	__	S.No. 46	11	Solution should have Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring, log inspection, application control and Recommended scan in single module or an in single agent	Requesting you to please rephrase it to "The solution should offer anti malware, firewall, Application Control, File Integrity Monitoring, Change Control, Host Intrusion and exploit prevention, Network Visibility and Micro-Segmentation based firewall, Virtualisation Security and cloud workload solutions in a single agent functionality to ensure optimal security and compliance for critical servers both on premise or cloud based deployments and the solution apart from allowing only authorised applications to run, should block any changes from being done to	Please refer Corrigendum No. 5

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						authorized applications, like DLL's, System files, registry etc., thus providing application threats. It should prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits protection."	
50.	Volume-II (Part-A)	5 Security functionalities and services	5.5 Host Based Intrusion Prevention System & Server Security	77	Solution should able to detect and protect from reconnaissance/inspection scans	For provide optimal security, requesting you to please rephrase to "Solution should support Signature as well as behavioural based detection. Solution should support policies creation based on – user defined, adaptive mode and learn mode. Solution should support firewall capabilities to directly block unwanted traffic. Solution solution should provide facility to create User defined signatures. Solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signature updates."	No Change
51.	NA	NA			Our understanding is proposed DNS & DHCP solution should have integration with directory services and also should have integration with other tools like SIEM, Servicesnow, Cisco ACI, Tuffin etc.	In projects like Smart cities, the volume of hardware and virtual devices connecting to the internet and to intranet networks has led to exponential growth in the number of IP addresses required, leading to significant operational challenges. As a result, the performance, reliability, scalability, Tracking and ease of deployment and administration of these services have become key strategic assets for which DDI plays an key aspect in Network Infra. Kindly accept below request: "Bidder has to provide dynamic, integrated and centralized management of IPAM with DNS and DHCP services in a single process, ensuring the highest level of quality and efficiency. Any change made to the IP structure is automatically populated and pushed to the DNS and DHCP servers, removing the chance for error and dramatically reducing time and effort for network administrators as three tasks are turned into one."	No Change
52.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.4. - Internet Firewall	22	The appliance should have minimum 8x1/10G port switch multi-mode transceiver from day one	For future Scalability purpose It is highly recommended to consider other connectivity options also like 40 G and 100 G as well as future expansion module that can provide these connectivity. Requesting you to please rephrase it to " The appliance should have minimum 8x1G Copper and 4x10 G Fiber port with trncereciver from day one and one expansion slot that should support connectivity on 1Gbps, 10Gbps, 40Gbps & 100 Gbps in future if required. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1"	No Change
53.	Volume-II (Part-E)	2.4. Internet Firewall	S.No. 5	22	Solution should support minimum 4 Gbps of NGFW / Threat Prevention real-world / production performance, scalable to 16 Gbps,	Asked throughput is at lower side considering to 8x10 G interfaces.Also NGFW through must be inline with other throughout like IPS. Hence requesting you to please rephrase it to "Solution should support minimum 4 Gbps of NGFW / Threat Prevention real-world / production performance, scalable to 20 Gbps, and IPS through put support minimum 4 Gbps and scalable to 20 Gbps in same appliance without changing the hardware. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1 "	No Change
54.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.4. - Internet Firewall	22	6. Firewall should support at least 18,00,000 concurrent sessions	Inline with asked interfaces and throughput along with scalability concurrent session is at lower side. Requesting you to please rephrase it to " Firewall should support at least 18,00,000 concurrent sessions and scalable to 15 Million concurrent sessions in same appliance without changing the hardware. In case there are no scalability	Please refer Corrigendum No. 5

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						option in the appliance then the scalable parameter to be factored from day 1 "	
55.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.4. - Internet Firewall	24	Product : Internet Firewall : Management :The management platform must be able to store record of 15000 user or more	Management appliance is sized based upon logs GB per day of Logs. Depending upon the size of firewalls being managed would request you to please rephrase it to "The management platform must be able to store record of 15000 user or more and should support 280 GB per day lof Logs."	No Change
56.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.5. - Intranet Firewall	24	2. The appliance should support at least 4x1G Ethernet Ports & 4 X 10G ports with multi-mode transceiver from day one	For future Scalability purpose It is highly recommended to consider other connectivity options also like 40 G and 100 G as well as future expansion module that can provide these connectivity. Requesting you to please rephrase it to "The appliance should support at least 4x1G scalable to 8x1G Ethernet Ports & 4x10G 8 X 10G ports with multi-mode transceiver from day one and It should have one expansion slots that support connectivity on 1Gbps, 10Gbps, 40Gbps/100Gbps in future if required. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1 "	Please refer Corrigendum No. 5
57.	Volume-II (Part-E)	2.4. Internet Firewall	S.No. 3	22	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory of minimum 128 GB	Requesting you to please consider it for better performance and concurrency "Proposed Firewall should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats and must not use proprietary Application-Specific Integrated Circuit chips. Any workaround this will not be acceptable. The appliance hardware should support memory of 128 Gb or better."	No Change
58.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.5. - Intranet Firewall	24	5. Firewall should support at least 25,00,000 concurrent sessions	Inline with asked interfaces and throughput along with scalability concurrent session is at lower side. Requesting you to please rephrase it to " Firewall should support at least 25,00,000 concurrent sessions and scalable to 30 Million concurrent sessions in same appliance without changing the hardware. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1 "	Please refer Corrigendum No. 5
59.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.4. - Internet Firewall	24	Product : Internet Firewall : Management :The management platform must be able to store record of 15000 user or more	Management appliance is sized based upon logs GB per day of Logs. Depending upon the size of firewalls being managed would request you to please rephrase it to "The management platform must be able to store record of 15000 user or more and should support 280 GB per day lof Logs."	No Change
60.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.2 General Requirements	53	VI. MSI should ensure security and compliance of applications and data by maintaining consistent network and security policies across on premise and CSP cloud. The network and security policies should follow Virtual Machines as it moves within and across CSP and on-premise Data Centre.	Request to Remove this Point as this is OEM specific. Security and network infrastructure are asked different at both On-prem DC's and Cloud DC & DR, then How security & Network policy could be same. Request you to let MSI decide best security & network policies as per industry standard at both the place. Local DC in each city is asked with only Firewall & IPS device whereas Cloud DC & DR is asked with HIPS, WAF & DDOS and application security kind of solution then how come same policy will work. Also let MSI decide the best way to failover the VM from local DC to Cloud DC with given SLA time frame.	No Change
61.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.2 General Requirements	53	IX. MSI will host all software hosted in local datacentre at Cloud DC-DR for continuous synchronization with it. In the event of disaster resulting in local data centre unavailable, the local data centre software should run from cloud supporting same functionality as in local data centre but for limited set of camera feed	OEM specific point. Request to remove. Let MSI device how they will manage the failover.	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
62.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.5 Service Management and provisioning	54	II. Cloud Management interface should have the ability to unilaterally provision and de-provision the specific IaaS services contemplated by the project via Web Portal, Command Line Interface and Web Services Application Programming Interface ("API"). All the communication for these purposes should be secured at transport level using SSL / TLS and or SSH.	This point is OEM specific. Request to kindly delete this point.	Please refer Corrigendum No. 5
63.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.6 User / administrative management	54	IX. The CSP should provide monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health	This point is OEM specific. Request to kindly delete this point.	No Change
64.	Corrigendum: Volume-II (Part-A)	__	S.No. 15	5	X. Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines.	This point is OEM specific. Request to kindly delete this point.	As per Corrigendum No. 4
65.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.7 Integration	55	XI. Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing	This point is OEM specific. Request to kindly delete this point.	Already addressed in Corrigendum No. 4
66.	Volume-II (Part-A)	4 Common Cloud based DC and DR	4.1.9 Security, Privacy and Compliance Requirement	56	IX. The CSP should provide a multi-tenant, Identity management (User Authentication & Authorization) and Directory service as a cloud service (as a native platform feature) backed by SLA. The Identity service should allow single sign-on (SSO).	This point is OEM specific. Request to kindly delete this point.	Already addressed in Corrigendum No. 4
67.	Corrigendum: Volume-II (Part-A)	__	S.No. 30	8	Should include storage virtualization /HCI software supporting all flash / hybrid nodes. It should work on mutually certified hardware of any vendor like dell, HP, Cisco, Lenovo, Hitachi etc. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.	All the leading HCI OEM have their own HCI/SDS software which is certified and compatible with their own hardware and current clause is favouring only one OEM. Moreover HCI vendors who have appliance based solution does not support intermixing any hardware from difference OEM's. In reality the SDS software vendor who does support this, does not recommend such architecture to avoid cluster balancing challenges Request to update below point for wider participation. "Should include storage virtualization /HCI software supporting all flash/ Hybrid nodes which runs on x86 hardware. Appliance Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM."	As per Corrigendum No. 4
68.	Volume-II (Part-A)	5 Security functionalities and services	5.3 Virtualization software	73	The solution should provide management of hardware system and the necessary functions required for discovering, bootstrapping, and monitoring the hardware, where it can access all hosts and switches on the out-of-band network.	Hypervisor or its Management tool cannot monitor the Hardware since Hardware comes along with their own Management Software. Request to update this point as below. "The solution should be able to dynamically allocate and balance computing capacity across collections of hardware resources of physical boxes aggregated into one	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						unified resource pool. Each node shall support out of band management. "	
69.	Volume-II (Part-A)	5 Security functionalities and services	5.3 Virtualizatio n software	74	The solution should provide for creation of complete application blueprints along with required virtual networking (routing, load balancing) and security services for the application using a user-friendly graphical interface by using drag & drop functionality	Request to update this point to generic requirement. The solution should have a multi DC application blueprint through which same predictable and repeatable deployment model is created. Thie application blueprint should translate to environment- specific API calls to provision compute, network, and storage resources; The solution should deploy the application components; manages the deployment, including run-time policies; and aggregates use and cost information.	No Change
70.	Volume-II (Part-A)	5 Security functionalities and services	5.3 Virtualizatio n software	74	The solution should provide true multi tenancy, each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines. At least 3 tenants will be required to be configured during the Cloud deployment	Kindly update this point for wider participation. The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute,network,storage ,applications and custom services through a unified multi-tenant IT service catalog	No Change
71.	Volume-II (Part-A)	5 Security functionalities and services	5.3 Virtualizatio n software	75	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi/ Hyper-V/ RHEV.	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi and Hyper-V/RHEV	No Change
72.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.7. - Blade Servers (Web, Application, Database, Platform Solutions etc.)	28	14. System Management: Should be able to provide Single console to manage Servers.	Request to update this point to current Generation Management systems. should be able to monitor blade and rack servers hosted across multiple locations through a single console. The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure.	No Change
73.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.7. - Blade Servers (Web, Application, Database, Platform Solutions etc.)	28	14. System Management: Power management tool – Single interface to optimize and control every usage	Request to update this point to current Generation Management systems. Power management tool – Single interface to optimize and control every usage. Tool should also be able to provide Automated hardware configuration and Operating System deployment to multiple servers with Zero-touch repository manager and self-updating firmware system.	No Change
74.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.7. - Blade Servers (Web, Application, Database, Platform Solutions	29	15. Remote Management: Should include Power Management, necessary licenses should be included.	Request to update this point to current Generation Remote Management systems. Should include Power Management, proactive security & software advisory alerts and provide an alert in case the system is not part of OEM Hardware Compatibility list. All necessary licenses should be included.	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
			etc.)				
75.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.7. - Blade Servers (Web, Application, Database, Platform Solutions etc.)	29	15. Remote Management: Should be able to monitor all systems components (BIOS, HBA's, NICs)	Request to update this point to current Generation Remote Management systems. Also, with Converged architecture there is no separate HBA & NIC card provided with the server. Remote Management: Should be able to monitor all systems components (BIOS & I/O cards), identify potential issues due to driver & firmware incompatibility and should provide anticounterfeit.	No Change
76.	Corrigendum: Volume-II (Part-E)	—	S.No. 75	14	Chassis should have enough redundant 20/25gb based converged modules / ports to provide a minimum FCOE uplink bandwidth of 40/50Gbps per blade server and 20/25Gbps sustained per blade server (with 1 module/port failure) for a fully populated chassis for converged Traffic.	Different blade vendors offers different architecture, Request to update this point as below for wider participation. Chassis should have sufficient number of redundant 25G based converged/FCOE modules to provide a minimum FCOE uplink bandwidth of 20Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure) for a fully populated chassis for converged Traffic.	Please refer Corrigendum No. 5
77.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.11. - Blade Chassis with Switch and Virtual KVM	35	9. Converged Module - The chassis should be provided with redundant modules for connectivity	With this change in corrigendum, DC Infra is prone to single point of failure as any bidder can take advantage of this clause and quote the blade solution with single connectivity module with multiple ports (considering as redundant). Please change it to original as below "Blade Support : The chassis should be provided with redundant modules for connectivity ."	No Change
78.	Corrigendum: Volume-II (Part-E)	—	S.No. 75	14	Chassis should have enough redundant 20/25gb based converged modules / ports to provide a minimum FCOE uplink bandwidth of 40/50Gbps per blade server and 20/25Gbps sustained per blade server (with 1 module/port failure) for a fully populated chassis for converged Traffic.	With this change in corrigendum, DC Infra is prone to single point of failure as any bidder can take advantage of this clause and quote the blade solution with single connectivity module. This changed point is favouring one OEM. Please change it to as below "Chassis should have sufficient number of redundant 25G based converged/FCOE modules to provide a minimum FCOE uplink bandwidth of 20Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure) for a fully populated chassis for converged Traffic."	Please refer Corrigendum No.5
79.	Volume-II (Part-C)	AI/Training/Analytics/GPU Servers		58		Analytics Server- Server should be configured with 2 no. of latest controllers, 32 GB GPU. Training- Server should be configured with 4 No. of latest controllers, 32 GB GPU or scalable.	No Change
80.	Volume-II (Part-D)	SAN Switch	74		SAN Switch	Specifications for SAN Switch is already given in Volume 2 Part A Central Scope Page No. 32 and it is confusing here. Request to delete it from here and if required in the Sultanpur Lodhi, bidder can refer those specifications for ease of understanding.	No Change
81.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.4. - Internet Firewall	22	6. Firewall should support at least 18,00,000 concurrent sessions	We have raised query to for concurrent session which was asked : "at least 18,00,000 concurrent sessions" in RFP Not addressed	Please refer Corrigendum No. 5
82.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.5. - Intranet Firewall	24	5. Firewall should support at least 25,00,000 concurrent sessions	We have raised query to for concurrent session which was asked : "at least 25,00,000 concurrent sessions" Not addressed	Please refer Corrigendum No. 5

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
83.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.6. - Network Intrusion Prevention System	27	8. The appliance should support a throughput of minimum 1 Gbps scalable to 4 Gbps within the same box and latency should be <50 ms for all kinds of real-world traffic/production performance in Active-Active or Active- Standby mode	IPS throughput should be at least equal or higher to Intranet firewall other it will be a serious bottleneck in overall design and will lead severly degradation of network performance. So request you kindly increase IPS throughput to 6Gbps from day one and scalable to 10-11 Gbps as per NGFW clause "6 Gbps of NGFW / Threat Prevention". scalability of IPS should be at least 50-70 % of asked throughput. latency on any security device is dependant on number of security rules and granularity of inspection rules. Thus it is not feasible to predict latency before actual deployment. so request to change the latency number to "low latency or ultra low latency word"	No Change
84.	Volume-II (Part-E)	2 - City Datacentre Active Infra Equipment's	2.6. - Network Intrusion Prevention System	27	9. The appliance should support minimum of 2,00,000 connections per second scalable upto 6,00,000 connections per second without changing the hardware	IPS connection per second number should be as per intranet/Internet Firewall number only. So request you to kindly change CPS should be between 25K-50K and scalability of 70-80K considering 50-70% scalability .	No Change
85.	Corrigendum: Volume-II (Part-A)	2. Virtual Firewall (v-NGFW)		17	Point no.-1 : The Virtual Firewall shall be entirely Software based for private/Public cloud environment and shall support cloud virtualization platforms such as VMware ESXi, Microsoft Hyper-V, KVM, Amazon AWS, Microsoft Azure, GCP etc and should have minimum 16 vCPU license from Day 1	Request to remove licenses dependency on vCPU as its OEM specific . Kindly updated it with required throughput and let OEM suggest required CPU for virtual firewall.	As per Corrigendum No. 4
86.	Corrigendum: Volume-II (Part-A)	2. Virtual Firewall (v-NGFW)		17	Firewall shall have feature of application visibility and application control with inbuilt SDWAN feature	Request to remove SDWAN as its OEM specific and not all OEM does it.	As per Corrigendum No. 4
87.	Corrigendum: Volume-II (Part-A)	2. Virtual Firewall (v-NGFW)		18	Should provide the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance	Request to remove this point as this is OEM specific. Different vendors have different mechanism to provide multiple admin access to make policy changes . As per best security practise management of all Firewalls be it virtual or Physical , on-prem or cloud should be using a single management.	As per Corrigendum No. 4
88.	Volume-II (Part-A)	NA			NA	From the RFP, we understand that the EMS solution is needed for all 3 Smart Cities (Amritsar, Jalandhar, and Sultanpur Lodhi) of Punjab. Please confirm if the deployment of these solutions will be done separately for all 3 smart cities or will it be single centralized deployment? Suggestion is to have Single Centralized deployment of EMS software for all 3 Smart Cities for Monitoring and Management of all smart city components across all 3 cities, having them private labled in EMS software to ensure security and privacy of data/information between the cities. If Amritsar personal will log into system, they can only view data for Amritsar and not for other 2 cities and same for other 2 cities. This saves a lot of cost, effort, time and also simplifies the management of solution.	No Change
89.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	26	1. Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise.	ISO 27034-1 standard helps organizations integrate security controls in the software through their software development cycle, by defining security frameworks & vulnerability management processes. This certification protects customer assets from potential cyber breaches & security threats while complying with the Application security standards. Hence request you to please revise the clause as follows:	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						"Enterprise Management System should from an OEM that is ISO 27034-1 & ISO 27001 certified to provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise."	
90.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	26	6. Solution should provide for future scalability of the whole system without major architectural changes.	Punjab 3 smart cities are major milestone for Government of Punjab and to ensure that the proven Smart City solution is chosen for the project, it becomes critical to ask for Smart City experience out of 30+ Smart city RFPs being already concluded in India. Hence request you to please revise the clause as follows: "6. The proposed Enterprise Management Solution should provide for future scalability of the whole system without major architectural changes. and must have at least 5 Smart City projects implemented or in execution phase."	No Change
91.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	26	7. Solution should be distributed, and scalable and open to third party integration.	To ensure that the proposed NMS/EMS is proven at the scalability required for the said project and is operational in the Indian Public Sector space and thereby avoid risk of being a test bed for solutions not known to scale up to the requisite levels. Hence request you to please revise the clause as follows: The proposed EMS Solution should be distributed, and scalable and open to third party integration and have at least 3 deployments in Indian Government/ Public Sector, monitoring & managing 10,000+ network nodes in each of such deployments. Customer names, solution details and OEM undertaking needs to be provided at the time of bidding.	No Change
92.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	27	8. The solution should be able to monitor all the IT assets for the organization across all the location spread across including servers, network, routers, switches etc.	Solution having been analysed & recognized by leading analysts ensures that an industry standard solution is being proposed. This is important because as EMS is the only solution that gives visibility into the project and is responsible for SLA measurements and audits, and therefore all the stakeholders must agree to the reports been generated from EMS. So at least asking for an ITSM tool which is used to generate SLA reports, to be recognized by leading analysts like ITC or Forrester will ensure a robust and matured solution is supplied by the bidder. Hence request you to please revise the clause as follows: "The solution should be able to monitor all the IT assets for the organization across all the location spread across including servers, network, routers, switches etc. and must be recognized by leading analysts (Forrester Wave/ IDC MarketScape) in ITSM reports for last 2 years."	No Change
93.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	27	14. The solution should provide network, server, application and database performance information and alarms and should be able to show it in a single console and provide a reporting interface for all network and system components.	EMS consists of multiple tools. Having all these tools from the same OEM will ensure that the components are pre-integrated and adequately tested and hence time to value realization is quick and issues of integration does not arise. Hence request you to please revise the clause as follows: "The proposed EMS solution should be an integrated, modular and scalable solution from single OEM with single support function across all the modules (i.e. all Network Monitoring, server Monitoring including application (Synthetic transactions, Real user experience, deep dive code level analysis) and database monitoring and Service Management tools should be from single OEM) to provide a single console and a	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						reporting interface for comprehensive fault management, performance management, traffic analysis and business service management, IT service desk\ help desk \trouble ticketing system & SLA monitoring functionality."	
94.	Corrigendum: Volume-II (Part-E)	—	S.No. 10	3	A11- 02 Common RFP - Vol-II Part-E (Corrigendum) S. No 10: PE IEEE 802.3af / POE+ IEEE 902.3at compliant	PE IEEE 802.3af / POE+ IEEE 802.3at compliant	Please refer Corrigendum No.5
95.	Volume-II (Part-E)	1 - Surveillance Components	1.6. - Industrial grade Field Layer-2 FE 16 port POE Switch	15	3. Switch should have minimum 200W PoE power available or extra power injector should be provided	3. Switch should have minimum 150W PoE power available or extra power injector should be provided	Please refer Corrigendum No. 5
96.	Corrigendum: Volume-II (Part-E)	—	S.No. 33	6	The switch should provide Minimum 16 port or 2 X 8 Ports of 10/100/1000 Mbps GE ports and 2 GE SFP uplinks Ports or more. Should be proposed with ruggedized transceivers as per solution. The switch shall be DC powered. Should support minimum 20 Gbps or more, full duplex wire rate switching throughput	The switch should provide Minimum 16 port or 2 X 8 Ports of 10/100/1000 Mbps GE ports and 4 GE SFP uplinks Ports. Should be proposed with ruggedized transceivers as per solution. The switch shall be DC powered. Should support minimum 20 Gbps or more, full duplex wire rate switching throughput	Please refer Corrigendum No. 5
97.	Corrigendum: Volume-II (Part-E)	—	S.No. 39	7	The switch should provide Minimum 16 port or 2 X 8 Ports of 10/100/1000 Mbps GE ports and 2 GE SFP uplinks Ports or more. Should be proposed with ruggedized transceivers as per solution. The switch shall be DC powered. Should support minimum 20 Gbps or more, full duplex wire rate switching throughput	The switch should provide Minimum 8 port or 2 X 8 Ports of 10/100/1000 Mbps GE ports and 4 GE SFP uplinks Ports. Should be proposed with ruggedized transceivers as per solution. The switch shall be DC powered. Should support minimum 20 Gbps or more, full duplex wire rate switching throughput	Please refer Corrigendum No. 5
98.	Volume-II (Part-A)	3.4 Minimum Technical Specification Software	3.4.1 Enterprise Management System (EMS)	37	90. The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	90. The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	Please refer Corrigendum No. 5
99.	Volume-II (Part-c)	6.7 Virtualization Software		47	Specification for Virtualization Software	Duplicity in the RFP Vol – II, Part A and Part C	Please refer Corrigendum No. 5
100.	Corrigendum: Volume-II (Part-A)	Virtual Security Information and Event Management		15	Specification for Virtual Security Information and Event Management	3 – 4 words / specifications are OEM specific. Mail received from XXX	Please refer Corrigendum No. 5
101.	Volume-II (Part-C)	6.21. Backup Appliance		57	Should support WORM feature for data protection & regulatory compliance. WORM feature shall support for point-in-time copies of a LUN or volumes with minimum performance impact.	WORM support is a legacy technology relevant for tape media as backup target device. In disk based appliance we have different architecture for protection against malicious or unintended backup data deletion. Request to change this clause to " Should support WORM or equivalent feature for data protection & regulatory compliance." for wider OEM participation.	No Change
102.	Volume-II (Part-E)	2.5. Intranet Firewall	S.No 4	25	Should support 6 Gbps of NGFW / Threat Prevention) real-world / production performance	Asked throughput is at lower side considering to 15000 users mentioned in point #26 also NGFW through must be inline with other throughout like IPS. Hence requesting	No Change

S.No	Document	Section No.	Clause No. (if any)	Document Page No.	RFP / Corrigendum Clause	Queries received from Bidders (Post release of Corrigendum 4)	Response to the Query
						you to please rephrase it to "Solution should support minimum 6 Gbps of NGFW / Threat Prevention real-world / production performance, scalable to 25 Gbps, and IPS through put support minimum 4 Gbps and scalable to 30 Gbps in same appliance without changing the hardware. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1 "	
103.	Volume-II (Part-E)	2.5. Intranet Firewall	S.No 6	25	Firewall should support at least 1,20,000 connections per second	Aske new connection per seconds is not inline with other components. Hence requesting you to please rephrase it to " Firewall should support at least 1,20,000 new connections per second and scalable to 4,00,000 new connection per seconds. In case there are no scalability option in the appliance then the scalable parameter to be factored from day 1 "	No Change
104.	Volume-II (Part-C)	6.21. Backup Appliance		57	Backup Appliance	Request to remove these specifications and generalize backup specifications as mentioned in Volume II Part B Amritsar (Page No 119) and Volume II Part D Sultanpur Lodhi (Page No 99) to have a common backup solution at all three locations.	No Change