Addendum No.1:

The following addendum is issued and shall be the part of the bid document:

In Volume 2 under Section 6.9.12, Outdoor Access Point and WLAN Controller stand deleted and the following are added.

Wi-Fi Access Points (AP)

Outdoor Access Point

1	The quoted wireless Access Point should be WPC-ETA approved
2	AP should be IP66 (or higher) certified. No third party casing will be accepted
3	Support 802.3 standard Power-over-Ethernet (PoE+/UPoE) with full capacity operation at full power of the radios
4	Must support Direct 100- 240 V AC/DC or PoE+ to power up access point
5	Minimum of 8 SSIDs available on each AP simultaneously without negatively impacting system performance
6	Access Point radio should be minimum 3X3 MIMO with minimum 3 spatial streams. Dual Radio capable.
7	Capable of supporting multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical 'touch' and no additional cost.
8	Real-time, fully integrated spectrum analyser capabilities on the APs, that does not require dedicated sensors or separate operating system running on the AP radios
9	The Access Point should have the technology to improve downlink performance to all mobile devices
10	Access Points must support 802.11ac from day one and backward compatible with 802.11n/g/b/a standards
11	For diagnostics, real time packet capture on the APs should be available, without disconnecting clients
12	Access point should be supplied with OEM mounting kit and shall support pole, wall, and roof mounting options
13	The Access point shall be rated for operation over an operating temperature range of 0° to 55°C or higher
14	For management, real-time, fully integrated spectrum analyzer capabilities on the APs should be available, that does not require dedicated sensors or separate operating system running on the AP radios
15	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio
16	AP should comply key International and Indian standards for safety, including RF radiations. APs must protect internally stored configuration information
17	To maintain consistent quality of service for users, network traffic should be prioritized according to applications/users and handled in the AP/Controllers or upstream devices so that critical traffic is processed immediately and network congestions are avoided

18	AP should have minimum one Auto-sensing Ethernet 10/100/1000 port
19	Connectivity wise, the AP should support 802.3 standard Power-over-Ethernet (PoE+/UPoE) with full capacity operation at full power of the radios

Indoor Access Point

1.	Support 802.3 standard Power-over-Ethernet (PoE) with full capacity operation at full power of the radios
2.	Access point should be supplied with OEM mounting kit for ceiling and/or wall mounting options
3.	The Access Point should have the technology to improve downlink performance to all mobile devices.
4.	Real-time, fully integrated spectrum analyzer capabilities on the APs that does not required dedicated sensors or separate operating system running on the AP radios
5.	Access Point radio should be minimum 3X3 MIMO with minimum 3 spatial streams or more on both bands. Dual Radio capable
6.	Access Point should be 802.11ac ready from day onefrom day one and backword compatible with 802.11n/g/b/a standards
7.	Minimum of 8 SSIDs and BSSIDs available on each AP simultaneously without negatively impacting system performance
8.	Real time packet capture on the APs, without disconnecting clients
9.	Capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical “touch” and no additional cost.
10.	AP should have minimum one Auto-sensing ethernet10/100/1000 port
11.	AP should have lock option for security

Wi-Fi Controller

1.	The WLAN controller should be, capable of managing at least 3000 Wireless APs from day one. It should be scalable up to a minimum of 6000 APs, as and when required. In case OEM/ bidder cannot provide WLAN Controller to support 6000 APs, multiple Controllers may be provided to meet the above mentioned requirement.
2.	System must be highly available and must have no single point of failure. Controller must be deployed in 1+1 redundancy with sub-second failover.
3.	Throughput performance should be 20 Gbps or more
4.	The proposed architecture should be based on Centralized Controller deployment model. AP’s should download OS and configuration from controller for improved security.
5.	The equipment should have MAC, 802.1x, web based authentication.
6.	The controller solution should facilitate monitoring, management, control, and up-gradation from the centralized Wi-Fi Management Centre.
7.	The controllers should communicate back and forth with the centralized security system

	and network management system in real time.
8.	The WLAN solution should have the hardware/software to implement advance WIDS & WIPS
9.	The systems should be able to detect malicious attacks, which can cripple down the public Wi-Fi system.
10.	The Wi-Fi Controller should be able to handle minimum 50,000 concurrent sessions. If required, multiple Controllers may be proposed to meet the requirement

Wired & Wireless Network Management System

1.	Manage all Access Points and Controllers proposed under this requirement.
2.	Provide real-time monitoring, pro-active alerts, historical reporting, efficient troubleshooting through centralized intuitive user interface
3.	Allow quick location of users and wireless devices for troubleshooting, planning and asset tracking, based on location of the connected Access Point.
4.	To ensure that new and existing wireless APs and controllers are automatically discovered anywhere on the network, the operations solution should support both upper layer discovery methods (i.e., SNMP and HTTP scanning) as well as Layer 2 discovery protocols.
5.	Provide client troubleshooting tools, including showing client Signal to Noise Ratio (SNR), Received Signal Strength Indicator (RSSI) and session throughput.
6.	Provide tools to help better manage RF coverage, address security issues, location tracking to provide a clear picture of who is on the network, their location and how the network is performing.
7.	Aggregate, correlate, alerts and logs wireless attacks that have been detected and reported on the network, providing a comprehensive picture of infrastructure.
8.	The operations solution should be able to determine the location of all potential rogue access points detected via wireless scans.
9.	Ability to use all authorized APs under management to perform wireless RF scans to detect unauthorized, 'rogue' access points, transmissions within range.
10.	Provide detailed performance statistics for WLAN equipment (statistics related with bandwidth, coverage etc.), also provide graphical details of WLAN utilization, average data rate, WLAN traffic etc. on a per AP basis.
11.	Provide easy-to-read graphs and reports showing how user signal quality, throughput, and other usage statistics have changed over days, weeks, months, and years.
12.	For faster problem resolutions, the operations solution should provide easy-to-use, real-time monitoring views of every device (i.e., access points and controllers) under management. For every device and radio, the operations solution should provide

	accurate information on number (and username) of connected clients, bandwidth utilization (in/out), device make/model/software version/serial number, frame and PHY statistics and errors (when supported by the device), IP address, MAC address, active alerts, event logs, etc.
13.	The operations solution should provide historical information (bandwidth, CPU utilization, memory, errors) for up to one year to surface any errors that could be masked by day-to-day or seasonal variations
14.	The operations solution should retain key client association session information (MAC and IP addresses, signal strength, location/roaming data, start and stop time, session length, bandwidth utilization, etc.) for at least one year to enable IT to perform intelligent network and capacity planning, diagnose problems, manage compliance requirements, etc.
15.	To facilitate service desk troubleshooting, user monitoring screens should provide 24-hour "playback" of a user's roaming patterns within a facility
16.	To accurately diagnose and resolve potential RF issues, network engineers and the service desk may need access to interface frame and PHY statistics and errors
17.	Certain types of alerts are more urgent or severe than others. The operations solution must allow IT to assign different severity codes to each alert type and to filter alerts by severity. Alerts must be capable of being sent via email. IT must also be able to specify which users will receive alerts and to determine how each alert will be delivered (email, network dashboard, etc.).
18.	The operations solution should have the ability to use all authorized APs under management to perform wireless RF scans to detect unauthorized, "rogue" access points within range. The operations solution should have the ability to ignore "neighbour" access points that are not managed but are not rogues (i.e., a legitimate WLAN established by a neighbouring organization within RF range).
19.	The operations solution should have a way to assess and classify threats to minimize the number of "false-positives" and to prioritize follow-up efforts. The classification scheme should be customizable to support our unique facilities and business environment
20.	The operations solution should be able to monitor IDS events as well as security

Edge Level Switch

- Minimum 4 port,10/100/TX PoE/PoE+ (May require higher port density at some locations, depending upon site conditions; and May require fiber ports at some locations, depending upon site conditions/distances)
- PoE Standard : IEEE 802.3af/ IEEE 802.3at or better
- Protocol Support :
  - IPV4,IPV6
  - Support 802.1Q VLAN
  - DHCP support
  - IGMP

- SNMP Management
- Should support Loop protection and Loop detection
- Should support Ring protection
- End point Authentication

- Operating Temperature : 0 – 55 degree C or better
- Equipment should be outdoor rated or industrial grade with minimum IP 20 rating
- Switch should be RoHS compliant

In Volume 2, add Section 6.10.4 after the end of section 6.10.3.

Smart Bin – Specification

Description	**Specification**
Capacity of Bin	2.5 cum
Density of waste	0.5 T/cum
Waste capacity of bin	1.25 Tons
Assuming Fill %	75%
Waste filled in each bin	0.94 Tons
Frequency of emptying	Alternate days
Waste to be emptied/ collected	235.52 TPD
No. of SUBs to be installed	50

BIN LEVEL SENSOR - Specification

- Enclosure : Polypropylene
- Shape & Dimension : cubical shape with max size of 100mmX80mmX50mm Or Mushroom shaped with max diameter of 100 mm & height
- Weight : Up to 450 gm
- Enclosure Protection : IP 67
- Operating Temperature : -20 C to + 80 C
- Power Supply : High performance battery
- Battery Life time : Approximately 5 years
- Built In Modem : GSM modem/shield for 2G or 3 G communication
- Level Sensor : Ultrasonic sensor with IP rating
- Range : 0.2 meter to 4 meter

In Volume 2, add Section 6.13 after the end of section 6.12.

i. Engaging STQC / CERT-IN Empanelled Agency for Audit

a) The SI will be responsible to engage STQC / CERT-IN Empanelled Agency to conduct the assessment/review for the system before rolling it out.

b) Specifically the STQC / CERT-IN Empanelled Agency shall look into:

- **Application audit shall include**:
  - Functionality audit *vis-a-vis* the Functional Requirement Specification (FRS) agreed upon during development phase
  - Determine systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc.
  - Review of database structure including:
    - Classification of data in terms of sensitivity & levels of access
    - Security measures over database installation, password policies and user roles and privileges
    - Access control on database objects – tables, views, triggers, synonyms, etc.
    - Database restoration and recoverability
    - Audit trails configuration and monitoring process
    - Network connections to database
- **Review of Network and Website will include:**
  - Penetration and vulnerability testing
  - Security exposures to internal and external stakeholders
  - Installation of requisite prevention systems like Intrusion Prevention Systems (IPS), etc.
- **Review and Implement of Security Policies and Controls will include:**
  - Review of backup process, including schedule, storage, archival and decommissioning of media
  - Physical access controls review (over DC and other critical area)
  - Review of change management process
  - Incident management process – covering identification, response, escalation mechanisms
  - Anti-virus (malware) controls – patching, virus definition file update
  - General computer controls review
  - Audit of IT Infrastructure will include monitoring the deployment of IT infrastructure at various locations including Data center and Disaster recovery center as per the BOM specified for the SI.
  - Performance / SLA Audit - whether the actual level of performance of the services is the same as specified in the contract of SI.

- Identify the key issues / bottlenecks in the system and will suggest the mitigation plans.
- Overall compliance to MSA and SLA - The compliance of the implementation partner with any other obligation under the MSA and SLA.