Request for proposal for Selection of Master System Integrator for Implementation of Smart Solutions in Lucknow.

Volume 2: Scope of Work

Table of Contents

1 PROJECT SCOPE OF WORK 4

1.1 PREPARATION OF THE PROJECT PLAN & DETAILED TECHNICAL ARCHITECTURE FOR LUCKNOW SMART CITY LIMITED: 6
1.2 REQUIREMENT GATHERING STAGE 7
1.3 DEVELOPMENT PHASE 8
1.4 FINALIZATION AND SUBMISSION OF A DETAILED TECHNICAL ARCHITECTURE 10
1.5 OTHER EXPECTATIONS FROM MSI 14

2 LEVEL 1: IMPLEMENT, VIEW & OPERATE 19

2.1 ENVIRONMENTAL SENSORS: 19
2.2 VARIABLE MESSAGE SIGN BOARD 23
2.3 CENTRALIZED COMMAND & CONTROL CENTRE 28
2.4 SITE PREPARATION FOR COMMAND CONTROL CENTER, 68
2.4.1 1.16.1 CIVIL AND ARCHITECTURAL WORK 69
2.4.2 FALSE CEILING 69
2.4.3 RAISED FLOORING 69
2.4.4 ELECTRICAL DISTRIBUTION SYSTEM 69
2.4.5 AIR CONDITIONING AND NATURAL CONVECTION 70
2.4.6 UPS REQUIREMENTS AND FEATURES 70
2.4.7 DIESEL GENERATOR SET 70
2.4.8 ELECTRICAL WORK FOR DATA CENTER (ON REQUIREMENT) 71
2.4.9 FIRE DETECTION AND SUPPRESSION SYSTEM 71
2.4.10 ACCESS CONTROL SYSTEM 71
2.4.11 CCTV SYSTEM 72
2.4.12 WATER LEAK DETECTION SYSTEM 72
2.4.13 BUILDING MANAGEMENT SYSTEM 72
2.4.14 RODENT REPELLENT 73

3 LEVEL 2: INTEGRATE & VIEW: 73

3.1 E GOVERNANCE: 73
3.2 ICT ENABLED SOLID WASTE MANAGEMENT: 74
3.3 SMART PARKING: 75
3.4 ENERGY EFFICIENT STREET LIGHTING SOLUTIONS: 76
3.5 INTELLIGENT TRAFFIC MANAGEMENT SYSTEM 77
3.6 ICT FOR CITY BUS SERVICES 78
3.7 CITY SURVEILLANCE 78
3.8 UP DIAL 100 80
3.9 INTEGRATION OF SCADA SYSTEMS (WATER SUPPLY, SEWERAGE PUMPING STATION ETC.) (FOR FUTURE INTEGRATION) 81
3.10 GPS TRACKING OF VEHCILES 81
3.1 UNIFIED SMART MOBILITY CARD: 82
3.2 BIOMETRIC ATTENDANCE SYSTEM OF SANITARY WORKERS 83

4 INTEGRATE, VIEW & OPERATE 84

4.1 GEOGRAPHICAL INFORMATION SYSTEM (GIS) & GIS CITY PORTAL 84
4.2 LSCL APP (MOBILE APP): 106

4.3 LUCKNOW SMART CITY WEBSITE: 107

5 COMMON COMPONENTS 113

5.1 CITY NETWORK 113
5.2 DATA CENTER AND DISASTER RECOVERY: 114
5.3 DATA SECURITY 145

6 OEM PROFESSIONAL SERVICES FOR PROJECT IMPLEMENTATION 161

7 HANDHOLDING AND TRAINING 163

8 PROJECT IMPLEMENTATION TIMELINES & DELIVERABLES: 166

9 MSI SCOPE OF WORK: 168

9.1 PROJECT MANAGEMENT 169
9.2 PROTOTYPE ACCEPTANCE AND FACTORY ACCEPTANCE TESTING 170
9.3 HARDWARE SUPPLY AND INSTALLATION STAGE 171
9.4 SOFTWARE DEVELOPMENT 171
9.5 SYSTEM INTEGRATION 172
9.6 TESTING 172
9.7 PILOT DEPLOYMENT 179
9.8 THIRD PARTY ACCEPTANCE TESTING, AUDIT AND CERTIFICATION 179
9.9 FINAL DEPLOYMENT AND DOCUMENTATION 182
9.10 OPERATIONAL SYSTEM ACCEPTANCE 183
9.11 COMPREHENSIVE MAINTENANCE FOR SYSTEM AND SERVICES 183

10 INTEGRATION OF FUTURE IT INITIATIVES 184

11 PAYMENT TERMS AND SCHEDULE 184

12 ANNEXURE 1: INDUSTRY STANDARDS 185

12.1.1 ANNEX-A (BIOMETRICS STANDARD) 185
12.1.2 ANNEX-B (DIGITAL PRESERVATION STANDARDS) 190
12.1.3 ANNEX-C (LOCALISATION AND LANGUAGE TECHNOLOGY STANDARD) 193
12.1.4 ANNEX-D (METADATA AND DATA STANDARDS) 196
12.1.5 ANNEX-E (MOBILE GOVERNANCE) 198
12.1.6 ANNEXURE-F (GIGW) 208
12.1.7 ANNEX-G (OPEN APIS) 214
12.1.8 ANNEX-H (INTERNET OF THINGS) 217
12.1.9 ANNEXURE-H (DISASTER MANAGEMENT) 220

13 ANNEXURE 2 (CONTROL & COMMAND CENTRE) 221

14 ANNEXURE 3: TEMPORARY LOCATION FOR COMMAND & CONTROL CENTRE: 241

15 ANNEXURE 4: LOCATIONS FOR ENVIRONMENTAL SENSORS 242

16 ANNEXURE 5 LOCATION FOR VARIABLE MESSAGE SIGN BOARDS: 243

17 ANNEXURE 6 FUNCTIONAL & TECHNICAL REQUIREMENT SHARED BY LMRC FOR UNIFIED METRO CARD244

1 Project Scope of Work

Lucknow Smart city Limited intends to select a Master System Integrator (MSI) for city of Lucknow by following competitive bidding process to design, develop, implement and maintain the Smart City System for a period of five years after Go Live date.

This document contains the following details:

a) Scope of work that will be assigned to the MSI as part of this project
b) Other terms and conditions of the envisaged Smart City System mentioned in the RFP document.

MSI will develop a Command & Control Centre as Integrated Smart City System for Lucknow comprising of below components/level:

1. **Level1: Implementation, View & Operate**
    1. Environmental Sensors
    2. Variable Message Sign Boards
    3. Integrated Command & Control Centre (ICCC)
2. **Level 2: Integration & View**
    1. E-governance (IGRS, PGRS, Property Tax etc.)
    2. ICT Enabled Solid Waste Management System
    3. Smart Parking (for future integration)
    4. Energy Efficient Smart Street Lighting Solution (for future integration)
    5. Intelligent Traffic Management System (for future integration)
    6. ICT for City Bus Services (for future integration)
    7. City Surveillance
    8. UP Dial 100

9. Integration of SCADA Systems (Water Supply, Sewerage Pumping Station etc.) (for future integration)
10. GPS Tracking of Vehciles
11. Unified Smart Mobility Card
12. Biometric Attendance System of Sanitary Workers
13. Any Other City Level Initiative.

3. Integrate, View & Operate

1. Geographical Information Systems (GIS) & GIS City Portal
2. LSCL App (Mobile App).
3. Lucknow Smart City Website (https://www.lucknowsmartcity.com)

Main objective of the project is to break Silos in the city with in the departments and across the departments. Also to install appropriate check points for solutions implemented, so that the services delivered to the public are at most satisfaction of public.

The bidders shall be responsible to carry out the detailed survey prior to submission of bid for the complete solution component requirement in order to finalize infrastructure requirement, network bandwidth, requirement, operational & administrative challenges etc.

The subsequent sections detail out the solution and scope with respect to each of the solution component. The MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. MSI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in this RFP and factor the same in its response.

More specifically, the following will be the activities to be carried out by the selected Bidder:

1. Project Planning, execution and Management.
2. Assessment and Gap analysis of requirement for all smart city components under scope.
3. Solution Design, System Customization and development for all components mentioned in this volume.
4. Survey and collections of the data for the various proposed components from the various stakeholders, authority will help in necessary documentation and support for getting the data required by the MSI.
5. ICT items Procurement, deployment and commissioning.

6. Site Preparation including required civil work (The MSI shall at the time of providing his feasibility report provide the list of civil infrastructure work required and provide a detailed estimate. The estimate prepared shall be as per the prevailing Schedule of Rates and for items not available in the SOR, Data Rate shall be worked out. The Client/Authority shall accord approval for the same prior to commencement of work), LAN Networking.
7. Application and general awareness Training
8. Business Process Reengineering for the selected applications/ services, if required
9. STQC Certification, It has to be carried out by MSI on his own cost before the GO-Live.
10. UAT & Go live
11. Capacity Building
12. Technical Support
13. Operation & Maintenance (O&M) for 5 Years after complete system go live date.

1.1 Preparation of the Project Plan & detailed Technical Architecture for Lucknow Smart City Limited:

After signing of contract, the MSI needs to deploy the team proposed for the project at site during development phase to ensure that a Project Inception Report is submitted to Lucknow Smart City which should cover following minimum aspects:

a) Project Charter, Project concept understanding
b) Names of the Project Team members, their roles & responsibilities
c) Approach & methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project)
d) Define an organized set of activities for the project and identify the interdependence between them.
e) Establish and measure resource assignments and responsibilities
f) Highlight the milestones and associated risks
g) Responsibility matrix for all stakeholders
h) Communicate the project plan to stakeholders with meaningful reports.
i) Measure project deadlines and performance objectives.
j) Detailed Project Plan, specifying dependencies between various project activities / sub-activities and their timelines.
k) Define Project Progress Reporting Structure which should cover the following parameters:

i. Cumulative deviations from the schedule date as specified in the finalized Project Plan
ii. Corrective actions to be taken to return to planned schedule of progress
iii. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI
iv. Support needed
v. Highlights/lowlights
vi. Issues/Concerns
vii. Risks/Show stoppers along with mitigation

After submission of the Inception report the MSI is expected to have an introductory meeting with all the stakeholders involved in the project for discussing the details in project implementation plan and the support required from the various stakeholder's in-terms of integration and implementation and data collection. The Lucknow Smart City Limited will arrange such types of meetings time to time on requirement basis.

1.2 Requirement Gathering Stage

The MSI shall conduct the detailed assessment of the business requirements and IT Solution requirements for Integrated Command & Control Centre as mentioned in this RFP. Based on the understanding and its own individual assessment, MSI shall develop & finalize the System Requirement Specifications (SRS) in consultation with Lucknow Smart City Limited. MSI will consult city SPV and other relevant stakeholders. While doing so, MSI at least is expected to do following:

i. MSI shall study and revalidate the requirements given in the RFP with Lucknow Smart City Limited and submit as an exhaustive FRS document.
ii. MSI shall translate all the requirements as captured in the FRS document into SRS.
iii. All the documents created for Lucknow City ICCC will be submitted to LSCL for review and approval.
iv. MSI shall develop and follow standardized template for requirements capturing and system documentation.
v. MSI must maintain traceability matrix from SRS stage for the entire implementation.
vi. MSI must get the sign off from user groups formed by Lucknow City SPV.

vii. For all the discussion with Lucknow Smart City Limited and its team, MSI shall be required to be present at Lucknow Smart City office with the requisite team members.

viii. Lucknow Smart City will provide necessary support for gathering required information and obtaining required data access for Present & future technical integrations of external systems with ICCC from other departments.

ix. MSI will prepare interoperability traceability matrix with third party systems (existing legacy systems with city ICCC) in consultation with Lucknow Smart City Limited and other relevant stakeholders (of external systems). Interoperability is an ability of one system to interact with another system. This matrix will cover all the use cases of system interaction and data movement.

1.3 Development Phase

The MSI shall carefully consider the scope of work and provide a solution that best meets the proposed Lucknow city ICCC requirements. Considering the scope set in this RFP, the MSI shall carefully understand the various prevailing Smart City solutions which are currently under implementation and envisaged in near future and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

A) Software Products (Configuration and Customization): In case MSI proposes software products the following need to be adhered:

i. MSI shall be responsible for supplying the application and licenses of related software products and installing the same so as to meet Lucknow Smart City ICCC requirements.

ii. MSI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.

iii. The MSI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The MSI shall report any exceptions to license terms and conditions at the right time to LSCL. However, the responsibility of license compliance solely lies with the MSI. Any financial penalty imposed on LSCL during the contract period due to license non-compliance shall be borne by MSI.

iv. MSI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the MSI shall supply:

- Software & licenses.
- Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.
- **System Documentation**: System Documentation both in hard copy and soft copy to be supplied along with licenses, document updates and shall include but not limited to following:
  - ✓ Functional Requirement Specification (FRS)
  - ✓ High level design of whole system
  - ✓ Low Level design for whole system / Module design level
  - ✓ System Requirements Specifications (SRS)
  - ✓ Any other explanatory notes about system
  - ✓ Traceability matrix
  - ✓ Technical and product related manuals
  - ✓ Installation guides
  - ✓ User manuals
  - ✓ System administrator manuals
  - ✓ Toolkit guides and troubleshooting guides
  - ✓ Quality assurance procedures
  - ✓ Change management histories
  - ✓ Version control data
  - ✓ SOPs, procedures, policies, processes, etc. developed for LSCL
  - ✓ Other documents as prescribed by LSCL.

- **Programs:**
  - ✓ Entire source codes
  - ✓ All programs must have explanatory notes for understanding
  - ✓ Version control mechanism
  - ✓ All old versions to be maintained

- **Test Environment:**
  - ✓ Detailed Test methodology document
  - ✓ Module level testing
  - ✓ Interoperability Testing
  - ✓ Overall System Testing
  - ✓ Acceptance test cases

- The above mentioned documents are required to be updated and to be maintained updated during entire project duration. The entire documentation will be the property of LSCL.

The MSI will be required to prepare the detailed technical architecture for the overall system, incorporating findings of Site survey exercise.

All the components of the Technical Architecture should:

(a) At least comply with the published e Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

(b) Be of leading industry standards and /or as per standards mentioned at Annexure –1

1.4 Finalization and submission of a detailed technical architecture

MSI shall submit the detailed Technical Architecture and description of each sub components, which should take into consideration following guiding principles:

- **Scalability** -Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in data centre equipment or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure) etc.

  The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data center infrastructure shall be capable of serving at least 1000 concurrent users.

- **Availability** - The architecture components should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote

failure, the systems need to be configured to mask and recover with minimum outage. The SI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core/data centre components level.

- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. The authority would carry out the security audit of the entire system upon handover and at regular interval during O&M period.

  Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI shall be required to repair / replace any equipment if stolen / damaged/faulty. Appropriate insurance cover must be provided to all the equipment supplied under this project.

  The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below.

  I. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
  II. The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
  III. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.

IV. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.

V. The overarching requirement is the need to comply with ISO 27001 standards of security.

VI. The application design and development should comply with OWASP top 10 principles.

- **Manageability** - Ease of configuration, on-going health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

- **Interoperability** - The system should have capability to take feed from cameras installed by private/Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.

- **Open Standards** - Systems should use open standards and protocols to the extent possible.

- **Single-Sign On-** The application should enable Single-Sign on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser based application accessed on the intranet, through Single-Sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system shall enable Single-Sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

- **Support for PKI based Authentication and Authorization-** The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital Signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.

- **Interoperability Standards-** Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in

future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

(a) At least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

(b) Be of leading industry standards and /or as per standards mentioned at Annexure –1.

All the personnel working on the Project and having access to the Servers / Data Center should be on direct payroll of the MSI/OEM/Consortium partner. The MSI would not be allowed to sub-contract work, except for following:

- Passive networking & civil work during implementation and O&M period,
- Viewing manpower at Command / viewing centres & Mobile Vans during post-implementation
- FMS staff for non- IT support during post-implementation

However, even if the work is sub-contracted, the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to city and approved by the Authority before resource mobilisation.

- **GIS Integration-** MSI shall undertake detail assessment for integration of all the Field level ICT interventions proposed with the existing Geographical Information System (GIS). MSI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Command Control Centers. If this requires field survey, it needs to be done by MSI. If such a data is already available with city, it shall facilitate to provide the same. MSI is to check the availability of such data and it's suitability for the project. MSI is required to update GIS maps from time to time.

- **SMS Gateway Integration-** MSI shall carry out SMS Integration with the Smart City System and develop necessary applications to send mass SMS to groups/individuals. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.

- **Application Architecture**

I. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/external factors. The standards should (a) at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

(b) Be of leading industry standards and /or as per standards mentioned at Annexure –1

II. The modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.

MSI shall design and develop the Smart City System as per the Functional and System requirement specifications finalized.

I. The Modules specified will be developed afresh based on approved requirement.
II. Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the Smart City System. These services will be processed through department specific Application in backend.

1.5 Other expectations from MSI

1. MSI shall engage early in active consultations with the Authority, other stakeholders involved and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
2. MSI is expected to recommend the proposed PMU Team for Lucknow Smart City Limited for Monitoring of the above projects alongwith their JD.
3. MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible

4. MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. MSI shall be responsible for supply of all the Products/equipment such as optical fibre cable, Network, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.
6. MSI shall be responsible for supply of passive components viz. Housings, Fibre Patch Cords, Racks etc.
7. MSI shall provide Warranty for all the IT hardware assets procured to comply with the requirements as defined in this RFP.
8. Validate / assess the re-use of the existing infrastructure if any with Authority.
9. Supply, Installation, and Commissioning of entire solution at all the locations.
10. MSI shall provide the bandwidth required for operationalizing each smart city initiative. The bandwidth requirement shall be analysed and procured by the MSI at its own cost / risk.
10. MSI shall install and commission connectivity across all designated locations if any required.
11. MSI shall ensure high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
12. MSI has to ensure secondary network services to meet the service level agreements.
13. MSI shall be responsible for up gradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority.
14. MSI shall ensure that the infrastructure provided under the project shall not have an end of life within 36 months from the date of bidding if required.
15. MSI shall ensure compliance to all mandatory government regulations as amended from time to time.
16. The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment,

accessories, patch cords (fibre), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.

17. Authority shall not be responsible if the MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.
18. All the software licenses that the MSI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements if required.
19. The MSI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The MSI shall ensure that all the OEMs have an understanding of the service levels required by Authority. MSI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.

    The MSI must attach OEM Authorization for the various products listed below.

    - Operating System
    - Virtualization layers
    - RDBMS
    - Integration Layer
    - Message Queue Layer
    - Application server
    - API Management Framework
    - All other OEM Enterprise Software products
20. Considering the criticality of the infrastructure, MSI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
21. MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.

22. MSI shall be responsible for setting up/ building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
23. Define and develop SOPs with the Client or its representative for the operations to ensure that ICCC systems are configured to support the operational procedures;
24. Creation of KPIs and dashboards as per the requirement of the LSCL;
25. Mobile version for the smart city platform for the LSCL;
26. Build and certify ICCC as per ISO 27001:2011 standards.
27. MSI is expected to provide following services, including but not limited to:

    i. Provisioning hardware and network components of the solution, in line with the proposed authority's requirements.

    ii. size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.

    iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart city initiatives.

    iv. Size and provision the internet connectivity for Service Provider network and Network Backbone.

    v. Liaise with service providers for commissioning and maintenance of the links.

    vi. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items

    vii. All equipment proposed as part of this RFP shall be rack mountable.

    viii. Authority may at its sole discretion evaluate the hardware Sizing document proposed by the MSI. The. MSI needs to provide necessary explanation for Sizing to the Authority

    ix. Complete hardware Sizing for the complete scope with provision for upgrade

    x. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.

xi. The MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.

xii. The MSI shall ensure that all active equipment (components) should support Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

28. The MSI shall directly interact with electricity boards for provision of electric supply at all desired locations including any Field Infrastructure solution mentioned in the RFP document. The Lucknow Smart City shall facilitate, if any documentation is required from its Side. The MSI will submit the bill for reimbursement on quarterly basis to the Lucknow Smart City Limited.

29. All existing road Signs which are likely to be affected by the works are to be carefully taken down and stored. Signs to be re-erected shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with City guidelines. Road Signs, street name plate etc. damaged by the MSI during their operation shall be repaired or replaced at the MSI's cost.

30. The infrastructure of existing systems or any other filed Infrastructure including the poles, cantilevers, aspects, controllers and cabling and associated mountings and civil infrastructure may need to be dismantled (where ever applicable) and replaced with the new systems proposed and shall be in the scope of MSI. The dismantled infrastructure shall be delivered at the Lucknow Smart City designated location without damage, at no extra cost.

31. Prior to starting the site clearance, the MSI shall carry out survey of field locations for buildings, structures, fences, trees, existing installations, etc. The Lucknow Smart City shall be fully informed of the results of the survey and the amount and extent of the demolition and Site clearance shall then be agreed with the LSCL.

32. Lightning Proof Measures

i. The MSI shall comply with lightning-protection and anti–interference measures for system structure, equipment type selection, equipment earthing, power, Signal cables lying.

ii. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall

have dustproof, antifouling, waterproof functions; capable to bear certain mechanical external force.

iii. Signal separation of low and high frequency; equipment protective field shall be connected with their own public equal power bodies; small size/equipment Signal lightning arrester shall be erected before the earthling.

iv. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment.

33. Any functionality not expressly stated in this document but required to meet the needs of the organization to ensure successful operations of the system shall essentially be under the scope of the MSI and for that no extra charges shall be admissible.

34. The MSI will setup a local server on the Integrated Command & Control Centre which will communicate with the central server.

35. The MSI will have to closely work with the LSCL Officials/State Data Centre Officials before the actual hardware and software deployment. The hardware and software related to data centre will be finally deployed after taking prior approval from LSCL/SDC officials.

2 Level 1: Implement, View & Operate

2.1 Environmental Sensors:

Overview: Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. As clear focus of building Lucknow as one of the finest example of smart city, Authority believes it is important that citizens know of the air that they breathe. Lucknow Citizens & visitors to City can enjoy unique experiences that keep them feeling good by knowing city's environment condition at different locations.

The Air quality should be monitored by a network comprising:

- fixed monitoring stations
- Data processing
- Data transmission to a central system
- A central processing system

Scope of Work

The Master System Integrator should:

1. Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations.
2. The environment sensors shall be integrated with the Lucknow Command & Control System to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc PM2.5, PM10, Noise Pollution, Electromagnetic Radiation etc. The data it collects is location-marked.
3. Various environmental sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.
4. Then this information is relayed instantaneously to Signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.
5. Further environmental sensors recorded data shall be used by Smart city Mobile application to enable user for alarm management and notification of environmental details on real time basis.

Components of Environmental Sensors:

1. **Wireless Environment Sensor**
   - Collect sensor data
   - Send recorded information to central system
2. **Central System**
   - Receive information from environment sensors
   - Display the information on real-time basis
   - Send information to mobile phone application
   - Save information in database
3. **Digital Display Unit**
   - Shall receive information from the central application System and operate accordingly

Functional requirement for Environmental Sensor:

- They should be ruggedized enough to be deployed in open air areas on streets and park
- They should be able to read and report at least the following parameters

Components	Air Quality Parameters to monitor and display

❖ Temperature ❖ .Humidity ❖ .Ambient Light ❖ Sound ❖ .CO ❖ NO2 ❖ Mosquito density	• NO2 upto 10ppm • CO upto 1000 ppm • SO2 upto 20 ppm • O3 upto 1000 ppb • PM 2.5 0 to 230 micro gms / cu.m • PM 10 0 to 450 micro gms / cu.m • Temperature 0 to 100 Deg. C • Relative Humidity upto 100% • Light upto 10,000 Lux • UV upto 15 mW/ cm2 • CO2 upto 5000 ppm

- The sensor should be able to communicate its data using wireless technology
- The data should be collected in a software platform that allows third party software applications to read that data.
- The sensor management platform should allow the configuration of the sensor to the network and also location details etc.

The standards for above should
(a) At least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and
(b) Be of leading industry standards and /or as per standards mentioned at Annexure –1.
(c) should comply with the guidelines and standards released by the central pollution control board time to time.

Technical Specifications:

S No.	Parameter	Specification
1	**Measurement elements**	Temperature, Humidity, Ambient Light, Sound, CO, NO2, O3, SO2, PM2.5, PM 10
2	**Measurement component** **Measurement range**	O3 : 0 – 390 ppb
		SO2 : 0 – 630 ppb
		CO : 0 – 31 ppm
		CO2 : 0 to 10% / 0 to 20%
		O2 : 0 to 10% / 0 to 25% (2 ranges each, maximum

		range ratio 1: 25 except O2) *Optionally, N2O and CH4 can be measured
		PM 2.5: 0 to 250 micro gms / cu.m
		PM 10: 0 to 450 micro gms / cu.m
		Light: up to 10,000 Lux
		UV: Proportion of UV Present in µW/Lumen & Total amount in µW/M2
		Noise: up to 100 dB (A)
3	**Temperature, Pressure and Humidity Sensor**	Real-time Temperature Range: outdoor 0ºC ~ 50ºC
		Real-time in Air Humidity Level Display
		Real-Time Pressure Display (in Bars or millibars)
4	**Communication media**	Wi-Fi, Ethernet or GSM (4G)
		Sensors must have provision to interchange between Wi-Fi or GSM systems easily
5	**Software and Data backup**	Backup measurement data for up-to 5 days in case of network failure or system maintenance cycles
6	**Mechanical Enclosure**	Single enclosure with all components inside or simplified mounting
7	**Data validity and stabilization**	Sensors must ensure data of sensors is valid and not require stabilization times in case of power outages less than 5 hours.
8	**Product origin and certification**	Must also qualify a minimum international standards on product certification such as CE, FCC and PTCRB
9	**Rain Water measurement**	in mm
10	**Repeatability**	±0.5% FS
11	**Zero Drift**	±1.0% FS max./week (±2.0% FS/week max. if range is less than 200ppm) ±2.0% FS max./month for O2 meter

12	**Respond Speed**	120 seconds max. for 90% response from the analyses inlet
13	**Display Area**	Display size of Environmental sensors should be 3x2 mtrs.
14	**Colour**	True Colour
15	**Brightness**	>8000 cd/m2
16	**Viewing distance**	>300 meters

2.2 Variable Message Sign Board

Overview: Variable Message Signboard (VaMS) shall be installed at identified strategic locations. The VaMS shall communicate information & guidance about traffic, diversions etc. to the citizens/public on the road. They shall also be used for showing emergency/disaster related messages as and when required. The MSI shall describe in detail the design, operational and physical requirements of the proposed Variable Message Signboards to demonstrate compliance with all the specified requirements in this RFP.

Scope of Work:

The VaMS unit shall be able to communicate with the Command Control Centre system using GSM Data/ Wi-Fi/ Ethernet/SMS Channel. GSM data channel (GPRS) / Wi-Fi/ Ethernet shall be used to send online messages and SMS channel shall be used to send configuration packets to configure the SIM. Ethernet port shall also be extended to ground level using necessary cables for local troubleshooting. Each unit shall be provided with a unique identification number and shall communicate with the Command Control Centre system.

VaMS shall be managed and operated from the Command Control Centre handled by a server where information in the form of data messages shall be fed in a manner to be displayed on a specific VaMS installed at a particular location or across all locations. The VaMS boards shall be viewable from a distance of 100m and various angles on the road. For installing VaMS Signboards, the SI shall provide Gantry with spans, as required at various locations (Single lane road, double lane road). Spans need to be specified depending on the number of lanes that need to be bridged. SI shall consider additional space for lateral clearance as well as a vertical clearance height as per NHAI (National Highway Authority of India) guidelines.

Minimum Technical Specifications of the Variable Message Sign Board:

S.no	Specifications	Minimum Requirements
1.	Source of light	High intensity LEDs
2.	Colour	True Colour
3.	Brightness	>8000 cd/m2
4.	Luminance Class	L-3 as per EN 12966
5.	Contrast Ratio	R2-R3 as per EN 12966
6.	Beam Width	B-3 as per should be wide angle B6 or B7 or B4
7.	Viewing distance	>300 meters
8.	Display capability	Alpha-numeric, Pictorials, Graphical & video
9.	Pitch	10 mm
10.	Display Front Panel	100% anti-glare.
11.	Language	Multilingual (English/Hindi) and all fonts supported by windows
12.	Auto Dimming	Auto dimming adjusts to ambient light level.
13.	In built Sensor	Photoelectric sensor
14.	Storage capacity	Minimum 100 GB
15.	Display Area	Display size of VMD should be 2.88m*1.92m
16.	Number of Lines &Characters	The number of lines and characters can be customized as per the requirement (Min 3 Lines & 10 Characters)
17.	Brightness & contrast	Controlled through software
18.	Display Driving method	Direct current control driving circuit. Driver card of display applies Direct Current Technology.
19.	Display Style	Stay on and flashing
20.	Connectivity	IP Based
21.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
22.	Integration	With Smart City Operations Center and service providers for offering G2C and B2C services
23.	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
24.	Battery	Internal Battery with different charging options (Solar/Mains)
25.	Power	Automatic on/off operation
26.	Casing	IP-55 rated for housing
27.	Operating conditions	0° to 55°C

Functional Requirements of the Variable Message Sign Boards: (VMS)

S.No.		Description
1	**System Requirements**	
	a	The system should be capable to display warnings, traffic advice, route guidance, air quality, traffic congestion, live journey time, alternate routes to destination, whether updates emergency messages and any other dynamic messages automatically from the cloud. For live journey time and congestion levels, VMS solution shall be capable to draw the information on its own and also take the data feed from the cloud (e.g. google cloud etc) and work in an automated fashion depending on GPS location of a particular VMS. The real time information can also be pushed manually from ICCC as well as system should capable to take the data from the cloud for display on the board.
	b	The system should also be capable to display warnings, traffic advice, route Guidance and emergency messages to motorist. Emergency messages can also be distributed to specific/all VMS board via secure mobile and tablet communication.
	c	The VMS should display text (multi lingual – Hindi & English) and Graphic messages using Light Emitting Diode (LED) arrays.
	d	The System should able to display failure status of any LED at ICCC
	e	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.
	f	The VMS workstation at the ICCC should communicate with the VMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VMS workstation should receive status data from the VMS controller.
	g	VMS controllers should continuously monitor the operation of the VMS via the provided communication network.
	h	Operating status of the variable message sign should be checked periodically from the ICCC.
	I	It shall be capable of setting an individual VMS or group of VMS's to display either one of the pre-set messages or symbols entered into the computer via the Control computer keyboard or by another means.

	J	It shall be capable of being programmed to display an individual message to a VMS or a group of VMS's at a pre-set date and time.
	k	A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of Signs shall be possible to assign for individual VMS or group of VMS's.
	l	It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, content of the message, date and time at which displayed message/picture starts and ends.
	m	The central control computer shall perform regular tests (pre-set basis) for each Individual VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access. VMS shall use 128 bit encryption to ensure downloads/transfer of files.
	n	Display should be CE, FCC, CB certified.
	o	VMS shall also be able to work individually providing real time information in an automated manner even in the case of connectivity loss between central server and LED Board.
	p	The digital media player/thin client on the LED display shall have minimum 4 GB, RAM and 16 GB flash memory with atleast 1.5 Ghz processor for playing rich content and for integration with sensors.
	q	VMS shall allow integration and independent working of road side sensors at the board level without use of a hub and spoke model/push model for dispatching data.
	r	VMS shall have an option to view latest content screenshot of every display on the centrally hosted VMS application at the ICCC. The system shall maintain the history of messages archived for future reference and analysis.
	Variable Message Sign board application	
	a	Central Control Software allows controlling multiple VMS (up to 10) from one Console.
	b	Capable of programming to display all types of Message/ advertisement having Alphanumeric character in English &Hindi and combination of text with pictograms signs.
	c	Capable of controlling and displaying messages on VMS boards as individual/group.
	d	Capable of controlling and displaying multiple font types with flexible size and Picture sizes suitable as per the size of the VMS.
	e	Capable of controlling brightness & contrast through software.

2	f	Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.
	g	Real time log facility – log file documenting the actual sequence of display to be available at central control system
	h	Multilevel event log with time & date stamp
	i	Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
	j	Location of each VMS will be plotted on GIS Map with their functioning status which can be automatically updated.
	k	Report generation facility for individual/group/all VMSs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other Customized report.
	l	Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMS unit.
	m	Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
	n	Apart from role based access, the system should also be able to define access based on location
	o	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access
	p	Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with Minimum outage.
	q	Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.
	r	System shall use open standards and protocols to the extent possible
	s	Facility to export reports to excel and PDF formats.
	Remote Monitoring	

3	a	All VMS shall be connected/ configured to ICCC for remote monitoring through network for two way communication between VMS and control Room to check system failure, power failure & link breakage.
	b	Remote Diagnostics to allow identifying reason of failure up to the level of failed Individual LED.

2.3 Centralized Command & Control Centre

Overview:

The Integrated Command & Control Centre shall serve as a shared space to host backend systems of various components of the Lucknow smart city proposal. It will be a common facility from where various smart components shall be operated and monitored such as smart Signals, smart vehicles, Smart street lights, smart parking, city Surveillance, solid waste bins & Vehciles etc. The core objective of establishing Command & Control Centre is to provide a common ICT facility for hosting the backend systems of various proposed Pan City smart components and to act as a central monitoring and management platform for the same. The key objectives of establishing the Integrated Command & Control Centre are as below:

- Platform for monitoring and managing traffic flows on the roads in the city and various other systems related to traffic management.
- Platform for monitoring operational and performance aspects related to public transport, parking, information dissemination, citizen service delivery, etc.
- Aggregation of various data feeds received from sensors/systems and further process information out of these data feeds to provide interface /dashboards for generating alerts and notifications in real time.
- Equip city administration to respond quickly and effectively to any incidents/ crisis Situation in city. The Integrated Command & Control Centre fortifies the coordination among multiple agencies in response to incidents/emergencies/crisis Situations.
- Integrated Command & Control Centre shall house various smart components, which shall use the data and intelligence gathered from operations of other elements so that civic services and emergency services are delivered lot more efficiently and in an informed fashion.

Scope of Work

- LSCL has identified a temporary location for setting up of Integrated Command and Control Centre; MSI should inspect the location and factor in the amount of work needed to build ICCC in the bid document. The Temporary Location of the control and command centre is mentioned in annexure 2.
- A temporary Command and Control Centre shall be implemented at Adjacent Building of Lucknow Nagar Nigam (Building is known as Bhopal House) for monitoring and management of all Lucknow smart solutions till the permanent ICCC is not ready for operations.
- MSI shall be responsible for complete installation of temporary command and control centre which also includes all civil, mechanical, electrical and interior works.
- MSI shall also be responsible for dismantling temporary command and control centre as and when final ICCC is finalized. Shifting of existing equipment from temporary to final location shall also be under the scope of MSI.
- Control and Command Centre has to be set up at the defined location also the control and command centre will be migrated to other location in the near future and same has to be done by the Master System Integrator at his own cost.
- MSI should provide a universal dashboard to view all applications in a consolidated manner.
- MSI should be able to provide Unified view for each Departments:
    - Solid Waste Management
    - Intelligent Traffic Management System
    - ICT for City Bus Services
    - Smart Electricity Meter and Water SCADA
    - Environmental Sensors
    - City Surveillance
    - Variable Message Sign Boards
    - e-Governance/Mobile App
    - Unified Mobility card
    - Any other Feeds as defined in this document or feed from Future Integration

- MSI should be able to project this information on the video wall
- MSI should also continuously monitor all the infrastructure/Servers/Routers/etc which has been built as part of this RFP

- MSI should setup a dedicated helpdesk to support the field infrastructure laid out as part of the RFP.

2.3.1 General Requirements:

❖ **Integrated Presentation:**

- The portal shall be designed to present Smart Parking, Transport Management, Solid Waste Management, and Vehicle Tracking Management and other already implemented and upcoming solutions data under one umbrella for an enhanced user experience and administrative control.

- **Key information visualization:**

- The smart components will generate various kind of operational and control data. The IT platform shall present the key information relevant and useful to the citizens and other stakeholders.

- **COST OPTIMIZATION:**

- The IT platform should be provided at an optimum cost. Cost can be optimized by leveraging the existing hardware and network infrastructure, cloud services, framework, and reusing software components. The Uttar Pradesh has an IT Platform with NIC in place with extensive infrastructure and framework, which may be leveraged. The selected bidder may suggest other cloud options too, which may be more cost optimized. The bottom line is the selected bidder will have to identify a solution at an optimum cost for the LSCL IT Platform.

- **MINIMUM DATA REDUNDANCY:**

- Data redundancy and data duplication should be kept at a minimum. Effort should be spent to figure out if some data can be accessed from an existing repository, rather than entering the data all over again and storing them separately.

- **BUSINESS INTELLIGENCE:**

- Users should be able to drill down and roll up information to have specific views, analysis and decision making. The IT Platform shall be designed to cater to the business intelligence requirements.

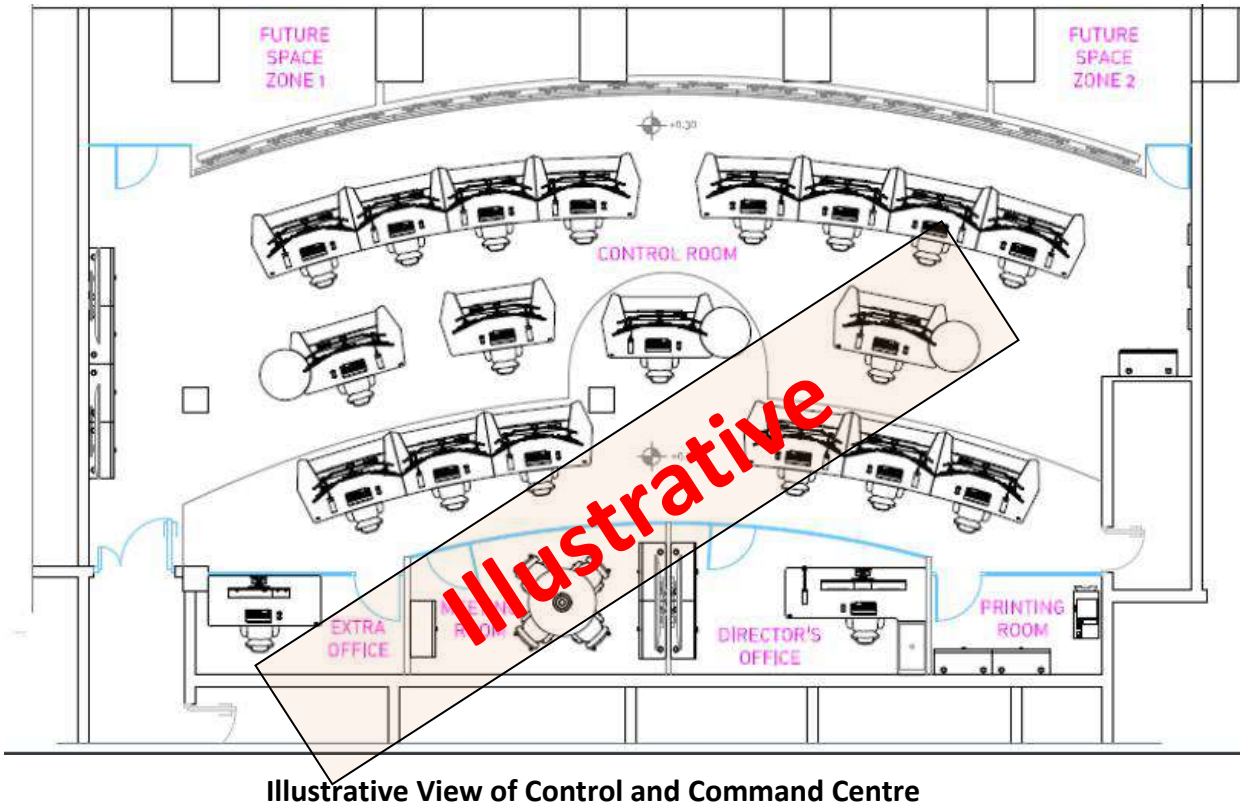
➢ **Web Portal & Mobile APP:**

- The portal functions/features shall be extended on to Mobile app also for reaching out to more users and providing quick access to the services. The portal must be designed for running on desktop, Tabs, Smartphone perfectly, as will be built with responsive design. The responsiveness provides acceptable appearance of the User Interfaces on various devices running in browser mode, but Mobile app has couple of advantages over running application in browser mode.
- The mobile app has to be developed for Android, iOS and Windows platforms. Instead of using native languages, hybrid language like phone gap may be used for developing the mobile app, for developing and maintaining a single code-base for the mobile app. The scope for the Mobile App will be a subset of the functional scope of the portal.
- The prime purpose of Mobile App is to provide flexibility for the citizens to access individual level information even if the user does not have access to a desktop computer at the time of need. The portal is primarily meant for the administrators/managers to access data at a gross level as well as individual level, and to perform some secured administrative activities.

➢ **PERFORMANCE VISUALIZATION**

- It is important to visualize performance of the smart components. Performance is normally judged by comparing target value for the Key Process Indicators (KPIs) and the actual values obtained. Currently the implementation of smart components (refer to the RFP of the Smart Components) does not support KPI and metrics calculation comprehensively. Hence performance visualization may be taken up in a later phase.

Indicative Layout of Control and Command Centre:



Illustrative View of Control and Command Centre

- Spacing should be provided for teams from different departments
- Design of the ICCC should be as per the ISO 11064 standards

Lucknow Integrated Control & Command Centre - Functional Specifications:

The Proposed Control & Command Centre should have IoT Platform Software (Data Normalization software) & City Operation Centre Software functionalities; All applications which will have field infrastructure like – Smart Water, Smart Transport, Smart Traffic, and Solid waste management etc, proposed to be integrate as part of Smart City initiative shall pass information processing via IoT Platform. IoT Layer must integrate lots of Services in the current scenario and must deliver an architecture which will be future scalable and can accommodate more Services/ Utility Solution Integration. IoT shall be a Common layer and is required for the **Normalization of the data** from different edge applications. This layer

will aggregate **and integrate utilities & sensors data** so as to ensure that **Device management**, **Analytics, Reporting, Dash Boarding** and **Integration of the Different Authorities data** can be performed from a Single operational screen. This layer shall also **integrate with different Independent Software Vendor (ISV) applications** Hosted at Data Center or at Cloud to provide the completeness of the solution. The Integrated command and control Centre platform shall be implemented in the form of a software system solutions comprising of a middleware, web portal, mobile app, several databases with specific purposes, and required applications for pulling in data, processing data and presenting data and run predictive analytics as and when required. The selected bidder has to deploy such platform for integration of all smart component/sensors use cases on this platform. The objectives of the IT platform are outlined below.

Scope of Work:

Functional Requirement of Command and Control Centre Platform:

The MSI has to provide, deploy and configured an integrated operations and dashboard application that integrated various Smart City use cases on this platform. Proposed Solution architecture should have combination of data collection, and normalization with below capabilities but not limited to. Command and control centre software should support cloud technology.

S.NO.	Functionality Description

S.NO.	Functionality Description	
1.	**Data Aggregation, Normalization and Access**	It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are- • Public Wi-Fi and Urban Service Delivery over Public Wi-Fi • Smart Outdoor Lighting • Smart Parking • Smart Traffic Management • Smart Energy Metering • Smart Water Metering • Vehicle Tracking System • Kiosks for Citizen Information • Citizen Interactive Kiosks for Urban Service Delivery • Environmental Monitoring • Smart Waste Management
2.		• The smart city integrated platform shall be able to normalize the data coming from different devices/instruments of various OEMs. • The City will be using various device vendors for various urban services. For example, in the Smart city journey of the city, various vendors of smart elements will be used for deployment and each will be generating data in their own format. This Smart City platform should be able to define its own data model for each urban service like parking, waste, lighting, transport etc. and map data from different device vendors to the common data model. This way, application development and analytics applications do not need to worry about the complexity of various data formats. • This data must be exposed to application eco system using secure APIs using API keys

S.NO.	Functionality Description	
		• The attributes of the API key(s) must restrict / allow access to relevant data, i.e. (the attributes can be like: specific domain(either parking or lighting or waste • Multitenant City operations Dashboard: City software platform Dashboard should display only relevant data (associated geographical data) for the user who logs in.
3.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, WiFi, IP Camera etc.
4.		The platform should also allow the manufacturers of the sensors to develop integrations themselves using various technologies without affecting the northbound applications and existing integration The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software and other applications
5.		The platform should be able to collect and normalize the data coming from different devices of same type (as environment sensors from various manufacturers etc.) and provide secure access to that data using data API(s) to application developers.
6.		The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control
7.	**Device Abstraction method**	The platform should normalize individual device data into Things Query Language or equivalent language to communicate among devices.
8.	**GIS Map Support**	System should support GIS mapping.
9.	**Location engine**	a) Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as

S.NO.	Functionality Description	
		unmapped facilities b) Geospatial calculation: calculates distance between two, or more, locations on the map c) Location-based tracking: locates and traces devices on the map
10.	**Service management**	a) Data brokerage, ID Management: Performs service management
11.	**Developer Program tools**	Sensor platform OEM should provide online Developer Program tools that help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. OEM should have technology labs via an online public facing web interface. These labs should be available 24X7.
12.	**Authentication, Authorization**	System should support standard Authentication, Authorization Performs
13.	**Data plan Functionalities**	Live data and visual feed from diverse sensors connected to the platform
14.	**API Repository / API Guide**	Normalized APIs should be available for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality.
15.		Platform OEM should have published the normalized APIs in their website for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform
16.		Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)
17.	**Platform upgrade and maintenance**	The OEM should be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration

S.NO.	Functionality Description	
18.		Platform should be able to be deployed on a public cloud for disaster recovery
19.	**Platform functionality**	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs
20.		User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions
21.		Application management: Provides role-based access view to applications
22.		Enabling analytics: Time shifted and real-time data available for big data and analytics
23.		The platform should also be able to bring in other e-governance data (SCADA systems) as i-frames in the command and control centre dashboard
24.		All of these data should be rendered / visualized on the command and control centre dashboard.

S.NO.	Functionality Description	

25.	**Control and Command Centre Operations**	• The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.
		• The solution should have the capability to integrate with GIS.
		• The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
		• The solution shall also provide an integrated user interface for all the smart elements implemented
		  • The solution should provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.
		  • The solution shall provide the “day to day operation”, “Common Operating Picture” and Situational awareness to the centre and participating agencies during these modes of operation
		  • It shall improve scalability for large and geographically distributed environments
		  • It shall provide complete view of sensors, facilities, e-governance/erp, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine
		  • It shall provide a uniform, coherent, user-friendly and standardized interface
		  • It shall provide possibility to connect to workstations and accessible via web browser
		  • The dashboard content and layout shall be

S.NO.	Functionality Description	
		configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard • The solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes • The solution shall be available via a VPN as a web-based interface or a thin-client interface • It shall be possible to combine the different views onto a Single screen or a multi-monitor workstation • The solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system • The solution should provide ability to extract data in desired formats for publishing and interfacing purposes • The solution should provide ability to attach documents and other artifacts to incidents and other entities • The solution is required to issue, log, track, manage and report on all activities underway during these modes of operation: • anticipation of incident • incident or crisis • recovery • incident Simulation
26.	**Integration capabilities**	This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices.
27.		Integrate devices using their APIs in to this platform.

S.NO.	Functionality Description	
		For example, if the City wants to deploy Smart Parking solution, this platform should have the ability and provision to write adaptors which interface with the parking sensors or management software of the parking sensors to collect parking events, data and alerts and notifications from the devices and their software managers.
28.		Platform should support on the fly deployment of Sensors. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown.
29.	**Edge Computing**	• Smart city platform should support standard edge appliances to connect industrial protocol devices (Edge appliance can be street level edge switches, routers, etc.) , Should support secure connection to edge devices, remote lifecycle management including software/firmware downloads and upgrades, remote management, self-registration, and local administrative interface. • Should support edge appliance to abstract downstream industrial protocols and upstream internet protocols. • Smart City platform should allow setting or changing the behavior on the edge through policies, which could be defined through cloud/on-premises instance of Smart City Platform. • Edge devices learn the behavior as analyzing the data to create better decisions with time. Share the outcomes with the smart city platform to impact other edges sensors/devices. • Smart city platform should support centralized Device Management for edge devices. • Smart city platform should support management tools to view, analyze, report on and modify the edge configurations.

S.NO.	Functionality Description	
30.	**Resiliency**	• This architecture provides the smart city use cases much needed resiliency while adapting cloud architecture • Provides ways to define policies that make applications or things respond to external environments • Schedule actions to happen at future time points • The smart city platform should have integrations with the network layer to proactively monitor any incidents on the network for active troubleshooting and triaging • The Smart city platform should be able to alert any incidents in the network proactively on command and control center • The Smart City platform should have demonstrated integration to collaboration tools to bring multiple stake holders and responders to respond an emergency or an urban services event.
31.	**API Based Open Platform**	• Provides urban services' API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system. • The smart city platform should have API Management capabilities like API Security, API Metering, and API Monetization. • The smart city platform is should be able to provide API access based on roles and access control policies defined for each user and the key issued to that user. • The vendor should have already documented different Urban Services APIs using which applications can be developed.

S.NO.	Functionality Description	
		• The vendor should be able to demonstrate existing applications that are developed using these urban services APIs.
32.		Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc.…)
33.		Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices.
34.		Provides urban services API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system.
35.	**Trending Service**	System should provide trends in graphical representation from data sources over a period of time. Trends should allow monitoring and analyzing device performance over time.
36.	**Policies and Events**	System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should a set of conditions that activate the behavior it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.
37.		System should provision to defines a set of conditions that can be used to trigger an event-based policy
38.	**Notifications,**	System should generate Notification, Alert and Alarm

S.NO.	Functionality Description	
	Alerts and Alarms	messages that should be visible within the Dashboard and on Officer Mobile App if required.
39.		All system messages (notifications, alerts and alarms) should always visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
40.		Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification.
41.	**Users and roles**	Users access to perform various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user should be associated with one or more roles and each role is assigned a certain set of permissions.
42.		These roles and permissions define the tasks that a user can perform. Additionally, system should assign one or more locations to each role so that the user can perform tasks at the assigned locations only.
43.		Roles and permissions define the tasks that a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. Each user should be associated with one or more roles and each role has an assigned set of permissions.
44.		The platform should allow different roles to be created and assign those roles to different access control policies.
45.		Since this platform is being used for managing Cities, the platform should also allow association of users and locations. For example, the platform should allow creation of locations in the system which correspond to various physical locations in the city and allow the admin to associate different users to different

S.NO.	Functionality Description	
		locations with the intent that each user can control only services for a location for which has been given access.
46.		System should support LDAP to be used as an additional data store for user management and authentication.
47.	**Service Catalog Management**	The Service catalog management module should allow categorizing the externalized and non-externalized services into logical groups by creating the service catalogs. In addition, system should allow manage the service catalogs by adding, modifying, or deleting the catalog details.
48.	**Reports**	The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. System should allow dashboard to generate reports and have provision to add reports in favorites list
49.	**Multi-tenancy**	1. Single instance of SMART CITY PLATFORM can be logically partitioned to host multiple tenants. 2. Each tenant should have respective administrator users. 3. Role based access control: Allows to provision users with specific roles to delegate monitoring and management of city resources based on regions (sub-boundaries in the tenant/City geography).Each Tenant can be further partitioned (zones/streets etc) with access to users for the respective zones/streets.
50.	**Global Market Presence**	Smart city suppliers should be adaptable to the emerging needs of cities. Suppliers should develop offerings that meet the growing interest in urban Internet of Things (IoT) applications, big data solutions, and the transformation in city approaches to energy

S.NO.	Functionality Description	
		policy, urban mobility, and city resilience.
51.	**Standard Operating Procedure**	Command & Control Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface. Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a Situation or carrying out an operation. The users should be able to edit the SOP, including adding, editing, or deleting the activities. The users should be able to also add comments to or stop the SOP (prior to completion). There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review. The SOP Tool should have capability to define the following activity types: • Manual Activity - An activity that is done manually by the owner and provides details in the description field. • Automation Activity - An activity that initiates and tracks a particular work flow and selects a predefined flow order from the list. • If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. • Notification Activity - An activity that displays a

S.NO.	Functionality Description	
		notification window that contains an email template for the activity owner to complete, and then sends an email notification. • SOP Activity - An activity that launches another standard operating procedure
52.	**Collaboration**	• The ICCC platform should provide an ability to bring multiple stake holders on to a common voice conference call as a standard operating procedure in response configured events • The stake holders can be on various types of devices like computer, smart phones, tablets or normal phones • The ICCC platform should have the capability to bring in multiple stake holders automatically into a common collaboration platform like persistent chat rooms and virtual meeting rooms in response to a SOP defined to handle a particular event. • The operator should also have ability create these collaboration spaces like virtual meeting rooms or chat groups manually. • The platform should allow the stakeholders to be notified of the creation of collaboration spaces using SMSs and announcements over PSTN telephone calls. • The platform must allow configuration of the policy under which such collaboration spaces are created and stakeholders are invited and notified. • The platform should allow stakeholders to share content relevant to the issue in the collaboration space. This content may include text; pictures, video, PDF/DOC/DOCX documents etc. and stakeholders should be able to view the content directly from the collaboration space.

S.NO.	Functionality Description	
		• The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration space. • The platform should allow stakeholders to participate in the web conferencing session using any means including smart phones, laptop computers, PSTN telephones, enterprise desk phones etc. • The platform should allow smart city devices (cameras, lights, various sensors etc.) to be added to the collaboration spaces. It should also allow the stakeholders to acquire data from such devices and to control such devices directly from the collaboration space, subject to access privileges for each user and device. • The platform should allow the stakeholders to access the collaboration spaces, participate in conversations, share content, create web conferences and control smart city devices from any endpoint (smart phones, laptops and other computers) and from any network location. • The platform should allow the stakeholders to be notified of the creation of collaboration spaces using SMSs and announcements over PSTN telephone calls. • The platform must allow configuration of the policy under which such collaboration spaces are created and stakeholders are invited and notified. • The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration

S.NO.	Functionality Description	
		space. • The platform should allow stakeholders to participate in the web conferencing session using any means including smart phones, laptop computers, PSTN telephones, enterprise desk phones etc. • The platform should allow the stakeholders to access the collaboration spaces, participate in conversations, share content, create web conferences and control smart city devices from any endpoint (smart phones, laptops and other computers) and from any network location.
53.	Enterprise resource planning (ERP) integration	System should allow integration of business process in ERP workflows like property tax collection etc.
54.		System should allow ERP data visualization at city dashboard
55.		The platform should have the capability to retrieve data directly from ERP systems. The APIs should be Restful and return the data in JSON format.
56.		The platform should also have the capability to read data directly from a set of databases (HBase, Mongo DB, Oracle, Cassandra, MySQL, Impala). To connect to any of the databases information on how to connect should be provided.
57.		System should be able to read data from flat CSV files.
58.	**Analytics Engine**	Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.

S.NO.	Functionality Description	
59.		The solution should be flexible to integrate with other city and government software applications.
60.		Analytics Engine module should have below intelligence capabilities; a) Advanced Predictive Analytics should be part of the solution. b) The solution should be flexible to integrate with other city and government software applications c) The solution should be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc. d) The solution should have predictions with measurable accuracy of at least > 70% e) The solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation. f) The solution should be robust, secure and scalable. The solution should have a visualization platform to view historic analytics
61.		The application should enable the customers to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks: a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results Predict outcomes
62.		Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel , NoSQL, RDBMS

S.NO.	Functionality Description	
63.		Analytics Engine should provide analysis of data from a selected data source(s). Analysis enables to define arithmetic and aggregation operations that result in the desired output. Analytics engine should provide capability to check analysis with multiple predictive algorithms
64.	Analytics Engine Visualizations	Analytics Engine should provide visualizations dashboard. In the visualization workspace it should allow to change visual attributes of a graph. User should not be allowed to alter the graph/visualization definition. In the visualizations workspace, user should able to do the following operations: a) Change the graph/visualization type b) Print the graph c) Export the graph d) Narrow down on the value ranges e) Toggle the axis labels Integrate with other 3rd party applications seamlessly. **The response time of the analytical tools used should be less than 10 sec.**
65.	**Export Formats**	System should allow export the analysis into min following formats: • XML/JSON • Excel • PDF • CSV
66.	**Cloud Infrastructure Operations**	**Hardened components:** The OS instances are hardened as per the latest CIS-CAT benchmarks with target of 80 % compliance. All actions are audit-logged. Hardened OS shall have only required applications, process and permissions. All components

S.NO.	Functionality Description	
		are hardened as per industry standards
67.		g) **Infrastructure components security:** Platform should support user encrypted storage volumes. Restrict inbound access from public network only on secure ports via DMZ proxy instances. SSH access is restricted with secure key pair and from designated jump hosts alone. User management and authentication is tied to Corporate SSO.
68.		d) **VM Infrastructure security:** Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure
69.	**Infrastructure as a Service support**	System should provider should support following security features • User encrypted storage volumes. • Restrict inbound access from public network only on secure ports via DMZ proxy instances • SSH access is restricted with secure key pair and from designated jump hosts alone. • User management and authentication is tied to Corporate SSO. • Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure Platform should have appropriate controls in place to detect source code security defects, functionalities for any outsourced software development activities from suppliers, open source libraries
70.	**API & Interface Security**	The access to data should be highly secure and efficient.
71.		• Access to the platform API(s) should be secured using API keys.

S.NO.	Functionality Description	
72.		• Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.
73.		Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where ICCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.
74.	**Data Security & Integrity**	• **Data Governance / RBAC:** Platform should support data governance & stewardship model, in which roles, responsibilities are clearly defined, assigned, implemented, documented and communicated • **Data Governance/ Resilient hosting:** Platform should have capability to restrict the storage of customer data to specific countries or geographic locations with resilient hosting options • **Data Protection / Production Data integrity:** Platform should support procedure in place to ensure production data shall not be replicated or used in non-production environment • **Data Protection / Data at rest:** Platform should support encryption for tenant data at rest (on disk/storage) • **Data Retention:** Platform should have capabilities to enforce tenant data retention policies • **Data recover & restore:** Platform should have capability to recover and restore data for a specific customer in the case of a failure or data loss. **Data disclosure & privacy:** Platform should disclose data attributes, elements collected from source. All the attributes should be disclosed & appraised to data owner. With appropriate approval from City authority, Platform should have ability to encrypt sensitive data

S.NO.	Functionality Description	
		element at rest.
75.	**Release Operations**	**Critical production assets:** Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses
76.		• **Patch Management:** Platform should have capabilities to patch vulnerabilities across VM infrastructure, applications and systems.
77.		• **Patch timeline/ notifications:** Platform vendor should provide risk-based systems patching time frames to tenants based on request
78.		• **Secure SDLC:** Platform should support automated source code analysis tool to detect security anomalies / defects in code prior to production
79.	**Scaling, Capacity Provisioning parameters**	• Platform should be scalable and should support capacity provisioning additional CPU, RAM to existing VM, Cloud infrastructure • Platform should have tools to monitors the healthiness of the individual tenants and status of CPU, Memory performance • The platform shall send alerts to the user once it exceeds certain limits in terms of CPU and Memory performance
80.	**Business Operations**	• **Audit & logging:** Platform should support centralized logging & auditing framework. Physical and logical user access to audit logs restricted to authorized personnel only.
81.		• **Legal/Supplier chain agreements:** Platform provider vendor should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs) between providers and

S.NO.	Functionality Description	
		customers
82.		**Critical production assets:** Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses
83.		**Outsourced SW Development:** Platform should have appropriate controls in place to detect source code security defects, functionalities for any outsourced software development activities from suppliers, open source libraries
84.	**Field Responder Mobile Apps**	Provide integrated Mobile Application for iOS, Android and Windows for capturing real-time information from the field response team using Mobile- Standard Operating Procedure.
85.	**High Availability**	• Platform shall meet availability level of 97.0 % for testing & development environment • Platform shall meet availability level of 99.0 % for Production environment
86.		• Platform shall have no Single point of failure. Software & hardware fault shall not result total system failure.
87.		All failure must report relevant error messages to the user
88.		Platform vendor shall provide supporting infrastructure, appropriate tools to measure & monitor system availability and automated notification for system failure and unavailability
89.		System response Time Measured as the elapsed time between the moment a user initiates a process using input device to last display of first screen • System response time should not exceed 3

S.NO.	Functionality Description	
		seconds for 2 concurrent users System response time for any web services shall not exceed 3 seconds for 100 concurrent users
90.	**Logging**	Platform should have logging frame with following functionalities • Logs shall readable in ASCII plaintext or UTF-8 format • All logs shall be time stamped • Log events shall capture user activities, applications, system & network IDPS messages • Centralized & secure log repositories to all log events • System logging shall be provided for all successful and unsuccessful login attempts and for all super user activities • Platform should implement mechanisms to trigger alerts and facilitate users to analyze and review logs efficiently • All critical logs are secured and sent to archive • Centralized logging shall be configurable to report for exceptions and generate reports based on desired filters • Logging framework shall be integrated with SIEM framework • Any anomalies shall be promptly identified & investigated through SIEM(Security Incident Management Framework) • Appropriate controls shall be put in place to ensure outage of the central log repository does not result in any loss of logs • The central syslog shall be able to normalize logs from wide variety of platforms / components to Common Event Format (CEF) to ease of use for monitoring and analysis and support logical data segregation so that the different user groups can only view their own

S.NO.	Functionality Description	
		managed equipment logs • Central syslog system shall have sufficient disk storage to keep the logs for 1 year to facilitate incident response investigation • Logging should have following retrieval time o Timeline : Log Duration o 6 Hrs : 0 – 30 days o 1 day : 30 – 90 days 5 days : Older than 90 days
91.	**Performance Monitoring Tool**	Performance monitoring tool shall include following functionalities • Identify infra and/or application components between the user and backend servers that is causing the problems • Providing key performance indicators • Identify the inter-dependencies between application & infra components • Able to provide network/ system node causing the problem • Provide email, SMS and/or mobile alert mechanism if performances falls below predefined thresholds Performance monitoring shall not adversely affect the performance of the platform
92.	**Database monitoring**	• Platform should provide database monitoring tool for DB health checks to monitor ❖ Memory allocation, usage and contention ❖ Disk I/O usage ❖ CPU usage for a particular transition ❖ Number of buffers, buffer Size and usage ❖ Active locks and locks contention, including waiting time ❖ Active users and status of their operations • List of users (complete or selected) with their access rights

S.NO.	Functionality Description	
93.	**Platform Environment**	• Platform provider shall have 3 environments 1. Development environment 2. QA environment 3. Production environment • All 3 environments shall be physically / logically separated All should have same system & application software versions
94.	**Platform Software**	• Platform provider shall provide complete information on all platform software deployed indicating clearly the software versions, quantity of licenses, functions, type of license (one time or annual recurring) • Platform provider shall transfer all licenses with maintenance service supports to authority There shall be no use of freeware, shareware and proprietary software
95.	**Backup and Recovery**	• Platform backup and recovery solution functionality shall meet following requirements ❖ Perform online database backup and recovery ❖ Support full, incremental, scheduled and on-demand backups ❖ Provide additional programs and utilities for the purpose of backup and recovery and administration ❖ Perform backup verification to ensure integrity of backup ❖ Perform automatic drive cleaning using pre-mounted cleaning tape ❖ Support the backup of all files including open files within servers including operating systems, database ❖ Be carefully administered and monitored

S.NO.	Functionality Description	
		Provide comprehensive reporting and analysis functions
96.	**Archival and Retrieval**	• Platform vendor shall propose a detailed housekeeping and archival strategy that meet the Authority's housekeeping policy and business requirements • The strategy shall enable the Authority to access historical data on an ad hoc basis for audit, verification and investigation purposes • Ease of restoration of archived data from online achieves or offline storage and it shall be able to keep track of all archival activities performed • Overall platform performance shall not be compromised during the archival process
97.	**Device Engine**	a) Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud b) Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine
98.	**Documentation**	• All application software developed shall be properly documented with header indicating title, author, date of creation/update, update description, abstract of program/ module, interfaces, description of variables and data structures • Platform provider shall maintain traceability matrices for all requirements, system design and testing. • The traceability matrices shall trace all requirements throughout all stages of development life-cycle • Full documentation and source codes of all the software programs, modules, algorithms, software engines, link interfaces, GUI that are designed, developed and/or customized by the

S.NO.	Functionality Description	
		contractor for the Platform shall be submitted to Customer
99.	**Incident Management**	• MSI has to provide an appropriate tools for incident and SLA management for the SLA Parameters defined in Vol. 3 of this RFP
100.	**SMS Gateway**	• ICCC solutions should have a SMS gateway for sending messages to citizens.

2.3.2 IoT Platform

In general, IoT Platform should have following functionality:

1) **Data Aggregation, Normalization and Access** - It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are-
    - Smart Outdoor Lighting
    - Smart Parking
    - Smart Traffic Management
    - Smart Energy Metering
    - Smart Water Metering
    - Public Safety and Safe City Operations
    - Connected Public Transport
    - Public Wi-Fi and Urban Service Delivery over Public Wi-Fi
    - Kiosks for Citizen Information
    - Citizen Interactive Kiosks for Urban Service Delivery
    - Environmental Monitoring
    - Smart Waste Management
    - Normalizes the data coming from different devices of same type (i.e. Different lighting devices, different energy meters etc.) and provide secure access to that data using data API(s) to application developers
    - The City will be using various device vendors for various urban services. For example, in the Smart city journey of the city, various vendors of smart elements will be used for deployment and each will be generating data in their own format. This Smart City platform should be able to define its own data model for each urban service like parking, waste, lighting, transport etc and map data from different device vendors to

the common data model. This way, application development and analytics applications do not need to worry about the complexity of various data formats.

- This data must be exposed to application eco system using secure APIs using API keys
- The attributes of the API key(s) must restrict / allow access to relevant data, i.e. (the attributes can be like: specific domain (either parking or lighting or waste etc. or combination of these), RO / RW /, specific to tenant (city, street within city etc.)
- Multitenant City operations Dashboard: City software platform Dashboard should display only relevant data (associated geographical data) for the user who logs in.
- The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, WiFi, IP Camera
- The platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software
- The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.
- The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control

Visualization/Control and Command Centre Layer

Control and Command Centre Operations - The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.

- The solution should have the capability to integrate with GIS
- The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
- The solution shall also provide an integrated user interface for all the smart elements implemented
- The solution should provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.

- The solution shall provide the “day to day operation”, “Common Operating Picture” and Situational awareness to the centre and participating agencies during these modes of operation
- It shall improve scalability for large and geographically distributed environments
- It shall provide complete view of sensors, facilities, e-governance/erp, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine
- It shall provide a uniform, coherent, user-friendly and standardized interface
- It shall provide possibility to connect to workstations and accessible via web browser
- The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard
- The solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes
- The solution shall be available via a VPN as a web-based interface or a thin-client interface
- It shall be possible to combine the different views onto a Single screen or a multi-monitor workstation
- The solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system
- The solution should provide ability to extract data in desired formats for publishing and interfacing purposes
- The solution should provide ability to attach documents and other artifacts to incidents and other entities
- The solution is required to issue, log, track, manage and report on all activities underway during these modes of operation:
    - ✓ anticipation of incident
    - ✓ incident or crisis
    - ✓ recovery
    - ✓ incident Simulation

Video Display Wall (VDW)	
❖	The VDW shall be provided as per the following requirements: 55” (Inch) each.
❖	Each of the above VDW shall be made up of DLP rear-projection cubes. Each DLP display cube shall measure 55 inches in diagonal. It shall include all controllers required for its operations.
❖	The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should have LED as its light source with ultra-thin configuration.

❖	It shall have an aspect ratio of 16:9.
❖	The light source lifetime of the LED shall be at least 80,000 hours.
❖	The brightness uniformity of the VDM shall be >95%.
❖	The Rear Projection Module shall have LED as its light source.
❖	The screen shall have adjustable low inter screen gap 1.00 mm or lesser to give seamless viewing experience.
❖	The Cube shall have redundancy in power supply, LED light source and its driver circuitry and its power supply
❖	The dashboard shall be capable of simultaneously displaying one (1) to one hundred (100) independent sets of information on the video display wall. Specific outputs to be displayed shall be chosen by operators.
❖	The VDW shall include video walls mounted close to each other to give a seamless viewing experience.
❖	Each cube of the VDW shall have its own IP address and on-board web server to provide standard information like status and health.
❖	The VDW shall be the primary visual information point to see CCTV videos, incident alarms, IoT screens, network health conditions, GIS maps, and any application running on city systems.
❖	The VDW shall provide a collaborative visual for operators and management to work and coordinate on various tasks in different situations.
❖	The VDW product selected shall be durable for optimal use over a long time in a 24/7 operational mode.
❖	The VDW shall provide image uniformity across the whole display area.
❖	The VDW shall have system availability with limited maintenance and low disruption of the operations room operations.
❖	The VDW shall be capable of displaying high definition (HD) and standard definition (SD) content.
❖	The VDW shall provide minimum viewing angles of: • Horizontal - ½ gain: ±35 degrees, 1/10 gain: ±57degrees • Vertical - ½ gain ±10 degrees, 1/10 gain: ±28 degrees
❖	Auto continuous-colour and brightness management mechanism to be
❖	The VDW shall have a user interface for all settings and operational parameters.
❖	The VDW shall support with enhanced brightness of at least 300 cd/m² to accommodate ambient light expected inside the room.
❖	The VDW units shall be new and current to the manufacturer's product line. The units shall not be discontinued products.

❖	Each VDW unit shall have front-access to the projection modules and internal components of the cubes for maintenance purposes.
❖	The brightness uniformity of each display cube and across the entire VDW shall be at least 95%.
❖	The video display cubes shall have anti-reflective screens in order to reduce reflection and glare on the display wall.
❖	The VDW shall not daisy chain video communications from one display cube to another. There shall be a direct video connection from the display content
❖	All video display cubes shall have a consistent image quality, automatic and continuous colour calibration and uniform brightness across the display wall.
❖	The VDW will have at least one (1) female DVI-I/HDMI input connector.
❖	The VDW shall have 10/100/1000 copper Ethernet communications port.
❖	A pedestal shall be provided to support the VDW. If the manufacturer's standard pedestal does not comply with the height requirement, the MSI shall supply a custom setup.
❖	The support structure shall be with a laminate finish.
❖	The support structure shall have open internal space for equipment.
❖	The support structure shall incorporate sound proofing to prevent noise penetration from the equipment/s into the operations room.
❖	The support structure shall have easy to open rear access covers.
❖	The MSI shall provide lateral support for the VDW. If fixations are required behind the VDW, the MSI shall propose and design an appropriate support system.
❖	The VDW pedestal shall be physically secured to the concrete floor of the building. It shall not sit on top of the raised floor.
❖	Each VDW projection engine shall be modular to allow sub-components to be replaced without disruption to other components.
❖	Each display cube shall not exceed a thermal dissipation of eight hundred (800) BTU per hour under normal operating conditions.
❖	The VDW shall allow for easy maintenance of modules, colour sync systems, etc. where downtime is no greater than twenty (20) minutes.
❖	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz. Power consumption of each cube shall be less than 300W.
❖	The VDW shall have an operational temperature between ten degrees Celsius (10°C) to thirty degrees Celsius (30°C).

❖	The VDW shall have a relative humidity of 20 to 80%, non-condensing or better.
❖	The VDW shall be of sufficient design, manufacturing and operational quality to provide twenty-four (24) hours, seven (7) days a week mission critical functionality.
❖	The VDW shall have redundancy of critical components like light module, drivers and power supplies.
Display Content Management System (DCMS) or Video Wall Management System	
❖	The DCMS shall include the VDW controller for the Operations Room VDW and a system to manage the visual content.
❖	The DCMS shall be able to display visual content on any network attached display device.
❖	The DCMS shall be able to input, manage, and distribute visual content, including digital CCTV video, web pages, CATV, workstation applications, and active screens from any networked workstation.
❖	The DCMS shall be able to decode, transmit, manage, and display the following formats of digital streaming video: • MPEG-4 • H.264
❖	The DCMS shall treat the VDW as a single display. It shall act as a single canvas with no pixel separation.
❖	The DCMS shall have the ability to create multiple spaces for different users to control display content. The DCMS shall be able to create a minimum of six (6) distinct operator controlled display areas. These display areas cannot cross over into another. The display areas can be created anywhere within the VDW.
❖	The DCMS shall be able to create display layouts for any sized display, including boardroom monitor and the operations room display. The DCMS shall be able to save a minimum of one hundred (100) display layouts for every display device within the ICCC.
❖	The DCMS shall be able to manage users and roles. The DCMS shall have an administrator role to have master control of all functions.
❖	The DCMS shall be able to separate the video wall into variable sized sections so that system defined users can manage only their portion of the video wall. Users not belonging to a particular group managing another portion of the video wall shall not be entitled to change layouts and sources.
❖	The DCMS shall be able to stretch, re-position, and resize any video source on any display device.

❖	The DCMS shall be supplied with a user interface (UI) independent of other systems.
❖	The DCMS shall have a seamless interface within the VMS UI of the CCTV. All DCMS interactions within the Video Management System shall be no more than three (3) mouse clicks to execute a DCMS function. The DCMS UI shall have the ability to run independently while the Video Management System is running.
❖	The DCMS shall be accessible on any networked workstation or networked monitor with OPS on the ICCC network.
❖	The DCMS shall be able to create and edit user groups. DCMS permissions for users and user groups shall be customizable. At a minimum the definable permissions shall include UI function rights, viewing access rights, source list access rights, and display access rights.
❖	The DCMS shall include an administrator role that shall be able to manage system configuration, sources, user groups, and user authentication.
❖	All users on the DCMS shall have a password-protected login.
❖	The DCMS shall be able to display a minimum of two hundred (200) independent visual sources simultaneously on the VDW in the Operations Room. The sources shall be of 4CIF resolution.
❖	The DCMS shall be able to display a minimum of twenty (20) independent visual sources simultaneously on all boardroom or auxiliary display device. The sources shall be of 4CIF resolution.
❖	The DCMS shall be able to create and add borders and text overlays to individual original video content source. The borders and text overlays shall have selectable options for colour, widths, text size, and flash on/off.
❖	The DCMS shall be able to display a minimum of ten (10) web browser applications without the use of screen capturing from an external network source.
❖	The DCMS shall be able to select and display any region of a multi-monitor display on a DCMS connected source. For example, if an operator has three (3) monitors, the operator can select monitors one (1) through two (2) for display on the VDW, while leaving monitor 3 for local display only.
❖	Visual content from networked sources shall be transmitted and displayed with no pixel loss or degradation.
❖	The DCMS shall be able to accept a minimum input of four (4) CATV video sources;
❖	The DCMS shall be able to control and manage all CATV tuners remotely from all video connected rooms in the ICCC;
❖	The DCMS shall be able to search for networked video sources.

❖	The DCMS workstation client software shall run on an industry standard-based operating system.
❖	The DCMS shall be able to run a minimum of twenty (20) workstation client software instances simultaneously.
❖	The DCMS shall have the ability to self-monitor and provide alerts to the administrator and designated users via e-mail.
❖	The DCMS shall have a SDK and API openly available without charge for future integration with third party applications.
❖	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
❖	The DCMS shall support 10/100/1000 Ethernet communications for device management and other communication.
❖	All DCMS hardware shall have an operational temperature between ten degrees Celsius (10°C) to thirty degrees Celsius (30°C).
❖	The DCMS shall have redundancy of critical components to support a twenty-four (24) hours, seven (7) days a week mission critical functionality.

Video Wall Management Software	
❖	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or schedule/timer based.
❖	The software should be able display multiple sources anywhere on video wall in any size.
❖	The software should enable the users to see the desktop of the graphics display wall remotely on the any PC or above connected with the DCMS and Video Wall over the Ethernet and change the size and position of the various windows being shown.
❖	The software should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the DCMS and Video Wall on the Ethernet.
❖	The software should copy the screen content of the workstation connected on the Ethernet with the DCMS to be shown on the Display wall in scalable and moveable windows in real time environment.

❖	The video wall management software should support open APIs to enable system integrators to integrate it with their Software. Multiple application programmer's interface (API) to facilitate third-party software to control and access Wall management software features including ability to query the available perspectives, launch sources in windows, switch perspectives, switch current window contents to available inputs for both networked or non-networked sources(on the input cards), query overall system status, and launch Applications.
❖	Key features of Video Wall management Software • Central configuration database • Browser based user interface • Auto-detection of network sources • Online configuration of sources, displays and system variables • Backup & restore capabilities • Scheduled backup • Advanced remote logging • Full resolution and full frame rate preview of all networked sources • Remotely monitor displays over the network with the actual preview of all sources shown • Drag and drop from sidebar to mini display for quick perspective changes • Integrated soft KVM for remote control of displays • Perspectives can be opened and shown on both workstations and displays alike • Standard and custom Tiling configuration • Share your perspectives with other workstations or displays
❖	Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes : • Switching the entire display wall on or off. • Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules. • Fine-tune colour of each cube

❖	The integrated view shall provide a database that • records all events • can record full status at given time intervals • can be exported to excel/html • show internal patterns
❖	Log file functions (full Audit trail capabilities) • Logs are not automatically overwritten ➢ Client logs ➢ Central server logs • Logs contain the following information ➢ Individual User ID that has control of the video wall at any given time ➢ Name of PC that has control of video wall at any given time. ➢ Time control was taken. ➢ Time control was released Time stamps in log shall be at the one (1) second interval, or less

2.4 Site Preparation for Command Control Center,

The LSCL will provide a building for set up of temporary command & control centre at adjacent building of Lucknow Municipal Corporation. The MSI shall provide the detailed design in all aspects for the design-build (including but not limited to civil, mechanical, structural, electrical, communications, fire, fit outs, furniture, etc.) for the interiors of the ICCC temporary Command and Control Centre and it shall be the responsibility of the MSI and be approved by the LSCL or its representative. All interior works of ICCC shall be modular in nature allowing expansions. The MSI shall have the required personnel on the team including architect, structural engineer, MEP (Mechanical, Electrical, Plumbing) etc. as needed for this design-build. At least two (2) options for the design-build shall be proposed for the ICCC. Interior layouts and material to be procured for the ICCC shall be approved by the Client or its representative.

The MSI shall be require for complete site installation and commissioning for ICCC which includes Operation Area with operator consoles and video wall, Large Board Room, Board Room, Cabins and

Rack Room, local server room etc as mentioned in the RFP document and as per the requirement in consultation with the Client and its representative but not limited to the following:

2.4.1 1.16.1 Civil and Architectural work

The scope for civil work in this RFP is to furnish the Command Control in all aspects. The furnishing includes but not limited to the following:

- Cutting and chipping of existing floors
- Trench works
- Masonry works
- Hardware and metals
- Glazing
- Paint work
- False flooring
- False ceiling
- Storage
- Portioning
- Doors and locks
- Painting
- Fire proofing all surfaces
- Cement concrete works
- Insulation

All material to be used shall be of fine quality ISI marked unless otherwise specified

2.4.2 False Ceiling

The MSI shall install the top false ceiling with 1’ 6” of space from the actual room ceiling. This false ceiling shall house A/C ducts (if required) and cables of electrical lighting, firefighting, and CCTV. Appropriate pest control measures shall be taken to keep pests at bay.

2.4.3 Raised flooring

The MSI shall be responsible for raised flooring and provide for suitable pedestal and under structure designed to withstand various static and rolling loads subjected to it in server racks. The entire raised floor shall have laminated floor covering and beadings on all sides of the panel.

2.4.4 Electrical Distribution System

The SI shall be responsible for proper and uninterrupted working and shall ensure this by having the Data centre power distribution system with redundancy at three levels:

- Two incoming HT feeder supply from different sub-stations. Even if one feeder is down, the other one keeps power available.
- Emergency Diesel- Generator backup on failure of both main feeders
- UPS system with battery bank for critical loads
- Connection between UPS system and the network switch racks shall be redundant. No single point of failure shall exist in the power connectivity between network racks and UPS system.

2.4.5 Air Conditioning and Natural Convection

Since Data center is a critical area, precision air conditioning system shall be exclusively installed to maintain the required temperature. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. The task of the SI shall include (but not limited to):

- Connecting the indoor unit with the mains electrical point
- Connecting indoor and outdoor units mechanically (with 18 G hard gauge copper piping)
- Connecting indoor and outdoor unit electrically

The air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage.

2.4.6 UPS requirements and features

UPS system shall provide a redundant power supply to the following needs:

- Servers and important network and storage equipment
- Access control, Fire Detection & suppression system and surveillance system

The system shall be automatic with power supply from the mains and automatic switchover to DG set as secondary source for the Data Center. The specifications of UPS are provided in this RFP.

2.4.7 Diesel Generator set

The diesel generator set shall be in N+1 redundancy mode where N = 1. Detailed minimum specifications of the DG set are provided in this RFP. The SI shall be

responsible for regular operations and maintenance of the DG set. The SI shall be responsible for but not limited to:

- Fuel
- Preventive maintenance
- Corrective maintenance
- AMC, if any
- Replacement of any parts etc.

2.4.8 Electrical work for Data Center (On Requirement)

The electrical cabling work (On requirement/as per the actual needs)shall include the following:

- Main electrical panel in Data Center
- Power cabling
- UPS distribution board
- UPS point wiring
- Power cabling for utility component and utility points etc.
- Online UPS
- Separate Earth pits for the component
- The MSI shall use fire retardant cables of rated capacity exceeding the power requirements of existing and proposed components to be used at maximum capacity.
- All materials to conform to IS standards as per industry practice

2.4.9 Fire Detection and Suppression System

The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards.

The facility is to be equipped with gas based (Suitable for Data Center environments) fire suppression system appropriately sized for the given size of the Data Center.

2.4.10 Access control system

The Biometric/Access card based Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only with appropriate door locks and controller assemble connected with BMS system. The system deployed shall be based on proximity as well as biometric technology for critical areas and proximity technology for non-critical areas.

2.4.11 CCTV system

The SI shall provide CCTV system within the Data center and Command and Control Center on 24X7 bases. All important areas of the Data center, Command and Control Center along with the non-critical areas like locations for DG sets, entry exit of Command Center, Entry and Exit of building premises need to be under constant video surveillance. Monitoring cameras shall be installed strategically to cover all the critical areas of all the respective locations and the feed of the CCTV system should be integrated with control and command centre.

2.4.12 Water leak detection system

The Water Leak Detection System shall be installed to detect any seepage of water into the critical area and alert the security control room for such leakage. It shall consist of water leak detection cable and alarm module. The cable shall be installed in the ceiling and floor areas around the periphery.

2.4.13 Building Management system

The Building Management System (BMS) shall be implemented for effective management, monitoring and integration of various components like Access Control System, fire detection system etc.

The BMS shall perform the following general functions including but not limited to:

- Building Management and control
- Data collection and archival
- Alarm event and management
- Trending
- Reports and MIS generation
- Maintenance and complaint management

The scope shall include designing, supplying and installation of Building Management System.

2.4.14 Rodent Repellent

The entry of rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However the SI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

- **Minimum Specifications of the Hardware of the Control and Command Centre:** The minimum specifications for the hardware of control and command centre are attached as annexure 2.

3 Level 2: Integrate & View:

For Integrate and Command level of work, MSI will be required to integrate already implemented services in the city and also scope to integrate services which are proposed to be implemented by any of the line departments, City Corporation or smart city SPV in near future.

3.1 E Governance:

Description: Various Mobile applications/Web Portals have been developed by the various departments. Authority has decided to integrate the below portal/services to the Lucknow Command & Control Centre.

Web Portal:

1. Integrated Grievance Redressal System
2. Public Grievance Redressal System
3. e-District (Municipal Services)
4. others city levels initiatives

Functional Requirements:

Master System Integrator will be required to integrate above mentioned web portal and mobile apps with Lucknow Command & Control Centre to receive real-time updates from the various portals of different department so that all the updates can be monitored from a Single place. The Integration of the above defined portals will be utilized in Analytical layer

to help administration monitor its services and do a better citizen centric planning. The system will do the analytics of the real time data available and generate meaningful reports which will help the city administrator for decision making also will implement the SoP to fulfil the use cases.

3.2 ICT Enabled Solid Waste Management:

Description: Solid Waste management or Waste disposal is all the activities and actions required to manage waste from its inception to its final disposal. This includes amongst other things collection, transport, treatment and disposal of waste together with monitoring and regulation. It also encompasses the legal and regulatory framework that relates to waste management encompassing guidance on recycling etc. This project envisages about installation of smart sensor based bins, installation of sensor based community bins and door to door collection of the solid waste across the city.

Concessionaire has been awarded the work for Solid Waste Management system in March 2017 by Lucknow Municipal Corporation. The concessionaire has started the door to door collection of the solid waste, user charge collection, and waste to energy generation. Currently a command centre has been set up by the Concessionaire for getting the real time status of waste collection vehicles, status of sensor based bins whether it is filled or not.

Functional Requirements: Solid Waste Management will be required to be integrated with Lucknow Command & Control Center to receive real-time feeds of the of waste collection vehicles, status of sensor based bins. These feeds will be utilized in Analytical layer to help administration monitor its assets and do a better planning and also will implement the SoP to fulfil the use cases.

S. No.	Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
01	**ICT enabled Solid Waste Management System**	❖ Monitoring of the smart waste management system web and mobile application real-time level information for containers as well as the automatic warning system which notifies when containers require attention. ❖ GIS based Real-time monitoring of solid

		waste collection vehicles. Geo tagged bins whether cleaned or not through GPS on vehicles, in case sensors are on C&D Waste. ❖ Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person). ❖ Track progress of waste management service requests against pre- determined KPIs. ❖ Integration with control room complaints and GIS map with analytic layer.

3.3 Smart Parking:

Description: Smart parking solution shall provide real time view to citizens about locations of parking lots and availability of parking spaces in the lots. Smart parking solution may use video camera based analytics, parking occupancy sensors or other sensor based solutions to determine number of vehicles entering and exiting parking lots and the occupancy/vacancy status of individual parking lots. Availability of parking slots will be made available through web and mobile app media.

Tender for Implementing Smart Solutions at three pilot locations is already published by Lucknow Smart City Limited, The Name of the these pilot underground parking locations are Jhande Park-Lalbagh, Dayanidhaan Park-Lalbagh & Jhandewala Park-Aminabad. Also, MSI has to ensure integration of all the parking locations at control & command centre as & when implementations of the parking locations will be completed.

Functional Requirements: As soon as the Developer/Integrator will complete the work of Implementing Smart Solutions at these underground parking locations, Master System Integrator in collaboration with the Developer/Integrator of Smart Parking Solutions has to integrate the existing applications and data of these parking locations to Lucknow Command and Control Centre, also will implement the SoP to fulfil the use cases.

S. No.	Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
01	**Smart Parking Solutions**	❖ Consolidates all Cities parking information onto a single operations platform. ❖ ICCC will be required to receive feeds on the status of

		parking across the cities which are managed by the Smart Parking command centre (feeds received from all the edge devices of the Parking Solution). ❖ These feeds will provide information of available, non-available parking slots, functional and non-functional parking slots. ICCC will be required to get video feeds from the parking areas on real-time basis on requirement basis. These video feeds will help monitor assets of department. All the information received will be required to be mapped on the GIS map. ❖ All the information received from the Smart Parking command centre will go into the Analytical layer which will help city in better planning and running of operations. ICCC should be able to trigger the commands/alerts (if required) to the respective command centre. ❖ Should provide parking availability, revenue collection information on dashboard, received from various sources on real time basis. ❖ The platform should be able to integrate any type of parking sensor irrespective of the technology used. For example, some parking Sensors might use RF technology like LoRa or ZigBee to communicate the data and events, some might use GPRS or some might use Wi-Fi. Some parking sensors might use infra-red based detection, some might use magnetic field based detection or combination of the both where as some might use a video camera to detect parking occupancy. Irrespective of the technology, the platform should be able to integrate with these devices and their software managers and provide the data from such devices in a normalized and standard based data models.

3.4 Energy Efficient Street Lighting Solutions:

Description: Electric street lights are essential elements of a municipal environment and services. They affect resident sense of safety while influencing a city's ability to create an inviting environment for business and tourism. The Project is intended to improve the quality and reliability of Lucknow City out-doors lighting and thereby enhances public safety and quality of life for Lucknow city residents and visitors. The Project is designed to

be a modernization of the City's 'outdoor lighting system, made possible by leveraging future energy cost savings resulting from a large scale conversion of the City's existing lighting system to LED technology.

Functional Requirements: MSI on-boarded under this RFP will be responsible for coordination with the implementing agency and further integration of implemented smart lighting solution in the city to Lucknow Control and Command Centre, also will implement the SoP to fulfil the use cases.

S. No.	Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)
	Smart LED Street Light	❖ The ICCC should aggregate various data feeds from light sensors and systems further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time. ❖ Provide single dashboard/reports of smart LED Street of lighting solution. ❖ ICCC should support lighting control like diming, switch on/off, group/individual control etc. ❖ Integration with GIS map with analytic layer. Developing heat map to identify areas which needs systematic improvement.

3.5 Intelligent Traffic Management System

Description: As a part of Intelligent Traffic Management, traffic Signals shall be made 'intelligent' in order to make the traffic flow smooth and efficient and to help police to take proactive/ reactive measures and ensure safe & smooth environment on roads. The Intelligent Traffic Management will include Adaptive Traffic Signalling, Red Light Violation Detection (RLVD) systems, Variable Message Signs (VMS), CCTV Surveillance Cameras. Public Address system, etc. at road intersections, public places, market places or other critical locations. Digital Signboards/ VMS will enable Command & Control Centre to communicate effectively with citizens and also improve response while dealing with exigency Situations. Pollution & environment sensors will gather data about pollution, temperature, rains and other identified parameters.

Functional Requirements: As soon as the Technical Service Provider of the Integrated Traffic Management will complete the work of Integrated Traffic Management project, The Master System Integrator who will be selected under the scope of work of this RFP has to integrate the Integrated Traffic Management Systems to Lucknow Control and Command Centre and also will implement the SoP to fulfil the use cases.

3.6 ICT for City Bus Services

Intelligent Transportation Management shall enable real time tracking of buses plying in the Lucknow city. This system shall also provide data to Passenger Information System on Estimated Time of Arrival (ETA) at next bus stops in real-time. The electronic displays at Smart bus-shelters shall display the ETA of the next bus, route information etc. The passenger information will also be available through a common website and a mobile app.

Functional Requirements: As soon as the Technical Service Provider of the Integrated Transport Management will complete the work of Integrated Transport Management project, The Master System Integrator who will be selected under the scope of work of this RFP has to integrate the Integrated Traffic Management Systems to Lucknow Control and Command Centre and also will implement the SoP to fulfil the use cases.

3.7 City Surveillance

Description:

The City Surveillance monitors citizens through strategically placed sensors around the urban landscape, which collect data regarding many different factors of urban living. From these sensors, data is transmitted, aggregated, and analysed by governments and other local authorities in order to extrapolate information about the challenges the city faces in sectors such as crime prevention, traffic management, energy use and waste reduction. A dedicated command centre has been established by the department of police under the flagship project named “Drishti”. Under the Project Total 280 cameras were deployed at 70

locations across the city in which department of police is monitoring the city through these cameras, also as a part of the project Automatic Number Plate Recognition (ANPR) Cameras were deployed at various locations of the city and they are used for e-challan in case of any violation of the traffic rules by the citizens.

Functional Requirements: City Surveillance System will be required to be integrated with Lucknow Command & Control Center by the selected System Integrator to receive real-time feeds of the camera installed by the respective department. These video feeds will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning, also will implement the SoP to fulfil the use cases.

Locations: There are total 280 cameras functioning at 70 locations under the project the locations will be provided to the successful bidder for integrating the feed into LCCC and for locating it on the GIS map.

S. No.	Services	Brief Scope for Integration (Scope is only illustrative and non-exhaustive)

	Drishti- City Surveillance	❖ ICCC will receive feeds of CCTV existing cameras and new cameras on real time basis. ICCC will be integrated with existing cameras and new cameras. ❖ Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources. ❖ Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence. Push the video feed to Drishti police control room. ❖ Should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple Remote Control center ❖ Display module should have capability to control multi-screened display wall in sync with operator console. ❖ Should support fixed type and PTZ camera. Control PTZ function from the screen to control the camera but with changing tile configuration each camera should be viewed with much lower resolution. ❖ The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location. ❖ Integration with GIS map with analytic layer and Should also be able to trigger the commands/alerts (if required).

3.8 UP Dial 100

UP 100' is the official name of the Uttar Pradesh Police Emergency Management System. Police Emergency Systems have been operational in the form of distributed district level 'Dial 100' systems till now, where public calls in police emergency situations are handled by Police Control Rooms established at the District level. UP 100 has been established to provide integrated emergency services relating to public safety across the State of Uttar Pradesh on 24x7 basis. A centralized contact centre has been established at Lucknow for

receiving all emergency calls directly from across the State, including remote rural areas. The centre receives not only the mobile or phone calls, but also responds to all other modes of communications like email, social media etc. More details on dial 100 are made available on the link: http://up100.uppolice.gov.in/en/pages/home.aspx

Functional Requirements: Dial 100 System for the Lucknow city will be required to be integrated with Lucknow Command & Control Center by the selected Master System Integrator to receive real-time feeds on emergency response management system of police department. These feeds will be utilized in Analytical layer to help administration monitor its services and do a better urban planning also will implement the SoP to fulfil the use cases.

3.9 Integration of SCADA Systems (Water Supply, Sewerage Pumping Station etc.) (For future integration)

Description: Lucknow Integrated Control & Command Centre will be required to integrate Water Management-System Supervisory control and data acquisition (SCADA) control room to get real time information's of the water management systems such as flow measurements in pipes, any kind of pressure drops (leakage), automatic on & off etc. ICCC should be able to map this information on the GIS layer and help authority monitor the water management of the city. ICCC should also be able to trigger the commands / alerts (if required) to the respective command centre. All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations, also will implement the SoP to fulfil the use cases.

3.10 GPS Tracking of Vehciles

Lucknow Municipal Coorporation oversees the civic functions consisting of solid waste management, water supply services, etc. Lucknow Municipal Coorporation has implemented GPS enables smart tracking system for its Vehciles. The Smart Tracking application shall provide visibility into monitoring of process for the various municipal vehicles.

Functional Requirements: MSI on-boarded under this RFP will be responsible for coordination with the implementing agency and further integration of implemented Smart Tracking System for Vehciles of Lucknow Municipal Corporation in the city to Lucknow Command and Control Centre, also MSI will implement the SoP to fulfil the use cases.

3.1 Unified Smart Mobility Card:

Project Description: A Universal Card is an electronic card with the same form factor as a magnetic stripe card. It is capable of emulating any magnetic stripe data (MSD) card that is stored either in the card, or on a smart phone that communicates with it. It benefits the consumer by consolidating their credit, debit, membership, loyalty, gift cards and other forms of MSD cards into one card. Certain universal card products also add an extra layer of security to protect their cards against theft. Lucknow Metro Rail Corporation (LMRC) has introduced smart card for Lucknow metro based on unified common card payment system, which shall be accepted across different services such as city buses, Bus Rapid Transit System (BRTS), parking facilities Recreational Services, Municipal Payments, Utility Payments, and Retail etc. within a Lucknow city. This card shall act as electronic money facilitating the travel payment and other payment needs of the users within Lucknow City. It also enables access to electronic payment infrastructure services to all strata of society and makes itself available at every corner of the city. It also aids in green travel initiative by enabling lesser travel by citizens for payment services other than transport services. The fare media shall be issued by Financial Institution (FI) on behalf of Lucknow Nagar Nigam

Project Status:

- Lucknow Metro Rail Coorporation has introduced a common mobility card on closed loop card system which is having provision of integration of 32 services. The Details of Lucknow Metro Card shared by LMRC is attached as annexure 6.
- Lucknow Municipal Corporation has also developed an online as well as PoS based payment system for the property tax. HDFC bank has provided the payment gateway and the data has been hosted in the NIC data centre. PoS machine is currently accepting the credit and debit card for payment of the property tax and these PoS machine is deployed at all the 8 zonal offices of the Lucknow Municipal Corporation.

Scope of Work: The MSI is expected to integrate the services of various departments into Lucknow Metro card so as to achieve the concept of One City-One Card. Below are the minimum list of the services/ departments that are expected to be taken for the integration:

Services to be Covered	Nodal Agency/ Department
Municipal Services Payments	Lucknow Municipal Corporation
Public Parking –On street and Off Street (including multi-level parking) in the city	Lucknow Municipal Corporation/ Lucknow Development authority
Utility (water) Payments	Lucknow Municipal Corporation

- MSI shall undertake complete Integration Responsibilities with LMRC card for the services mentioned above, whereas LSCL shall facilitate such integration by providing any documentation support required to achieve the objectives.

- Any additional hardware required for LMRC card for Municipal Services payment will be procured separately by LSCL MSI has to recommend the compatible device for the payment services.

- MSI has to integrate the other services with the LMRC metro card for their payment system as and when required.

3.2 Biometric Attendance System of Sanitary Workers

Currently, the Sanitary Supervisors are collecting the attendance of the Sweepers working under him/her manually and the same is being updated to Lucknow Municipal Coorporation. However, it is learnt that the manual attendance system is not affective hence LMC has taken initiative on end-to-end solution by envisaging AADHAAR Enabled Biometric PoS based Hand Held Device project wherein, the genuine Sweepers working in field identification is determined by authenticating his/her biometrics.

Lucknow Municipal Coorporation is going to implement the AADHAAR based biometric Attendance system through Handheld devices for Sanitation workers in the Control of Sanitary Supervisors with reporting to Sanitary Inspectors along with necessary Software both server side & HH device side. The attendance will be taken ward wise at the work

location and updated immediately from the field using GPRS/4G Networks on a daily real time basis. Attendance will be calculated based on number of Shifts attended by the worker and will be consolidated for the entire month.

Functional Requirements: As soon as the IT agency of the Lucknow Municipal Coorporation will complete the work of Aadhaar Based Attendance System, The Master System Integrator who will be selected under the scope of work of this RFP has to integrate the Biometric Attendance Management System of Sanitary Workers to Lucknow Control and Command Centre and also will implement the SoP to fulfil the use cases. The Integration of the Biometric Systems will be utilized in Analytical layer to help administration monitor the services offered by its employees and do a better planning.

4 Integrate, View & Operate

4.1 Geographical Information System (GIS) & GIS City Portal

MSI would analyse the integration of all mentioned Smart elements in the RFP with Lucknow Smart City GIS maps and provide operations that help achieve KPI's mentioned in the RFP for each of the Smart elements. Base data has to be taken from GIS city portal on ArcGIS Platform and then the MSI has to analyse the gap in the GIS data and shall augment the GIS data as per the requirement. MSI should conduct analysis of integration points and provide a detailed report and get approval from LSCL before integration. LSCL will help MSI get the details from each line department and facilitate to get the required information on time. MSI shall develop operational procedures using GIS Map Interface. Also, it has been decided by the authority that the existing data of the GIS application will be hosted in the State Data Centre Lucknow. Later MSI is expected to migrate the GIS data to centralized data centre of LSCL which is located in State Data Centre MSI shall carry out existing setup study, analyse risk & business requirements, and carry out SRS by considering performance, scalability & other necessary factors. Submit SRS & architecture document for approval, Hardware, Network & related system design document should be submitted for approval

MSI shall carry out data integration requirement study with stake holders and submit SRS

(System Requirement Study) and Architecture document for approval by considering following factors (not limited to):

- Best GIS practices shall be followed in spatial positional accuracy, GIS layers overlay matching accuracy, data correctness and completeness
- All the generated, stored, linked data shall be available as necessary to integrate with City GIS Portal through web services or data sharing through live/real time, offline, periodical, etc. as deemed to be appropriate
- Apart from ICCC data, all other required data for city GIS Portal shall be carried out with suitable data design and data modelling
- All required Data Modelling, Design shall be carried out by MSI to get Design Document approved from client
- Integration, Export & Import of various formats of data such as KML, JSON, XLS, XML, etc. with external systems
- 3D Data of city

i. MSI shall carry out collection of data from various agencies or Government departments. Data creation - Necessary Survey, collection from various sources, compilation, digitization, accurate geo-referencing, migration, data conversion, integration & maintenance shall be carried out by MSI. Authority will help in providing the authorizing letters for collection of the data.

ii. GIS Map should be used as a common platform across all the solutions including Smart parking, Environmental Sensors Monitoring, Intelligent Traffic Management, Smart Street Lights, E-Governance, Utility Management system etc.

iii. Appropriate geo referencing & geo tagging on the map should be done covering all relevant Smart elements in the RFP and various POI's such as public amenities, bus stops, bus routes, bin locations, transfer stations, street poles etc.

iv. The component mapping should be multi layered keeping in vision the requirements for next 20 years.

v. GIS data modal need to be designed in accordance with Smart City solutions and need to be scalable and robust in nature so that it can meet any future need of smart solution and integration with future smart solutions and modules of city

vi. Alert, Events, Statuses for each smart element including hardware and software should be displayed on GIS Map.

vii. The related Smart elements like Variable messaging system should also be displayed in the same layer for the application. Ex: Smart Parking, Traffic Management,

Environmental monitoring, all the details should be real time by integration with Variable Messaging System.

viii. All government buildings and spaces should be geo tagged for the City of Lucknow.

ix. GIS data modal integrated should support domains, subtype, spatial rules and relationship, joins and spatial references etc.

x. GIS catalog should be used to manage and maintain the GIS data modal. It must support database administration for user creation and management for GIS database

xi. There must be grievance reporting functionality that is associated with ward. This interface must allow citizens to enter the description and detail about the grievance that can be submitted to respective city authority.

xii. GIS Maps should also display grievances status for all the Smart elements geo tagged on the Map

xiii. There must be proper workflows for authority /administrators to manage, approve and reject the request from public crowd sourcing.

xiv. GIS system must allow administrator to manage the citizens submitted grievance reporting and request from public crowd sourcing interface.

xv. Department specific search & query module should produce relevant output

xvi. SWM Assets mapping on GIS such as bins, transfer stations, landfill, garbage collection sites etc. Authority will provide Solid Waste Management System related data.

xvii. GIS maps must be integrated with GPS devices to locate real time position on GIS map & provide optimal route mapping There must be various analysis and work operations for Solid waste management from GIS application such as Geo fencing of waste bins, Geo fencing of vehicles, locate bins and bins location, signals, CCTV Surveillance cameras and provide planning & route optimization.

xviii. MSI to maintain, upgrade, integrate and enhance the City GIS portal application and GIS platform that is going to be developed under the GIS initiative of Lucknow Smart City Limited.

xix. MSI to design and develop the GIS based integrated application for Municipal departments and other departments.

xx. 8 Core Arc GIS Server on Active-Active mode along with two Desktop advanced are already existing and the MSI shall evaluate the sizing as per their requirement of the system and also has to maintain the existing city portal and the upgrade system for 5 years.

Proposed Technology under GIS initiative by Lucknow Smart City:

S.no	Description	Specifications

01	**GIS Application Server**	(2U Rack Server with dual Intel Xeon E52637 v4 processor, 64 GB RAM, 2*1 TB HDD, Windows Server 2012 std. Dual Port Fiber HBA.
02	**Database Server**	(2U Rack Server with dual Intel Xeon E52637 v4 processor, 256 GB RAM, 2*1 TB HDD, Windows Server 2012 std. Dual Port Fiber HBA.
03	**SAN Storage**	Dual Controller, Fiber Channel based storage with 16TB(8*2TB HDD), Scalability to 24 drives within the same enclosure
04	**Arc GIS Desktop Advanced**	2 unit
06	Server Rack & Accessories.	

Note: Above hardware and Softwares are tentative in nature and the final deployment of the above mentioned hardware and Softwares for GIS services will be done after the approval of the authority. The hosting of the application and database server of GIS is proposed on the state data centre.

xxi. Data creation - Necessary Survey, collection from various sources, compilation, digitization, accurate geo-referencing, migration, data conversion, integration & maintenance shall be carried out by MSI.

xxii. Responsible for identifying Data Gaps & take necessary measures & tasks to complete the data

xxiii. Existing data of Lucknow City GIS portal shall be verified for accuracy, completeness & correctness. Any shortcomings shall be rectified or updated with appropriate measures.

The proposed modules of the City GIS portal which is going to be developed under GIS initiative of Lucknow Smart City Limited are as below:

Portal	Modules	Functionalities

Citizen Portal	Map Visualization Module	- Base map based on available layers - Esri Basemap (topo, street, Satellite imagery) - Master Plans - Vulnerability Zone - Utility Network - Admin boundaries (LDA, LMC, Ward, Zone) - Transportation - Revenue / Parcel Maps
	Search Module	Search
	Tourism Module –	Tourism (based on Story Map concept)
	Location Based Information Module	Category wise information retrieval - Education - Community Services - Culture - Health/Family - Sports and Recreation - Security - Emergency - Govt. offices
	Tools	Basic tools for Map navigation - Navigation - Bookmarks - Measure - Print (Hardcopy or PDF) - Route / Directions
	Know your Ward	Thematic representation of the ward level boundaries
	Education	School level information as available from DISE and Query
	Health Services	Info of the Health Systems
	Public Feedback	Feedback form

GIS map will be provided by LSCL on ArcGIS for integration along with the available hardware & software. MSI to augment the existing GIS platform and application. All the smart

elements should be integrated with the GIS Map. The Master System Integrator is expected to review the existing base data from the city GIS Portal and analyse the gap in the GIS data and shall augment the GIS data and the city GIS portal as per the below requirement

Sl. no	Portal	Modules	Functionalities	
1a	Citizen Portal	Map Visualization Module	- Phase 1 Maps - Dept. Maps	Updated maps for the layers included in Phase 1 (if any) Map layers as made available by multiple departments/utilities
1b		Transport	Transport	City Bus Shelters, Bus Routes and Timings
1c		Tourism Module – 2	Tourism (based on Story Map concept)	Tourist information for the 199 heritages / tourist spots identified and documented. (Shown as POIs) – along with Pictures and description

1d		Location Based Information Module	Category wise information retrieval - Education - Community Services - Culture - Health/Family - Sports and Recreation - Security - Emergency - Govt. offices	Health Services Bus Stops, Bin Location (from), Utilities – service centers, Offices, Locations (from Utilities) Events (organized by Govt Depts., LMC, LDA, etc)

Sl. no	Portal	Modules	Functionalities	
1e		Culture & Community Events	Creation and upload of Events, Event Details, Calendar	Event locations and details – Auditorium, Hotels, Stadiums, Schools
1f		Tools	Basic tools for Map navigation - Overlay KML / CSV / XLS - Share Link (mail/Social Media)	All Maps. Functionalities like Overlay KML and Share- link will be customized and will be provided as required.

1g		Public Announcement	RSS Feeds Web Announcements	RSS feeds functionality will be customized so that users would be able to get updates; also there will be “Web announcements” on the public portal, like “One Map”.
1h		Population Query (Know your Ward) Census / Demography module	Thematic representation of the Census 2011 data from EB level to Corporation level	Boundary details from EB to Corporation along with linked Census information
1i		Land Information	Viewing of the Land Parcel information, query / view, (Phase 1 – only display and query on Plot number)	Parcel boundaries from Bhulekh / web services (no MIS info available. Need to mention the dependencies for integration)
1j		Health Services	Info of the Health	Data on the location and the

Sl. no	Portal	Modules	Functionalities
			Systems/services and Query
2	Water Supply Network Management	Asset Management	View and Query existing Water network (Pipes, Valves, fitting, etc.)

3	Sewer Network Management	Asset Management	View and Query existing Water network (Pipes, Valves, fitting, etc.)
4	Storm Water	Asset Management	View and Query existing Water network (drains, ducts, outlets/drop points)
5	Emergency Response	Incidence Management	• Incident Reporting • Incident Monitoring (Dashboard)
6	Feedback	Department Feedback	Feedback form for Department specific issues

Portal	**Modules**	**Functionalities**	
Integrated Command Centre	Integration with Smart City Central Command Centre	- Map display for the entire area - Operations Dashboard	- Incident feed containing information on the incident and agencies
Planning & DSS	Solar Energy	Site Suitability analysis	
	Solid Waste Management	Site Suitability analysis	

	Transport	New city Bus routes / stops planning Road Widening Cycle tracks / Walkable roads	
	Urban	Tools to support 2D / 3D Area based development	Area maps, proposed development plans
	Disaster management	Tools to support Preparedness, Response and Recovery operations	
Security / Surveillance	CCTV Integration	Location of the cameras and near real-time feeds	Camera locations, video /live feeds as a web service
Property Tax	Integration with Property Tax module of LMC	- Tax collection information - Tax status (updation)	Required information as web service
Water Supply	Operations	Control room operations –	Network data, Field Crew

Network Management	Management	Logging, Analyse of Incident, field crew notification, asset operations, asset status reporting, incident Monitoring	location, Asset Information

Sewer Network Management	Operations Management	Control room operations – Logging, Analyse of Incident, field crew notification, asset operations, asset status reporting, incident Monitoring	Network data, Field Crew location, Asset Information
Storm Water	Operations Management	Control room operations – Logging, Analyse of Incident, field crew notification, asset operations, asset status reporting, incident Monitoring	Network data, Field Crew location, Asset Information
Emergency Response	Event Security planning/management	• Security Planning • Field personnel updates • Field Ops center/monitoring	
Crowd Sourcing	Geo-enabling My City My Pride App		

Citizen Portal	Map Visualization Module		Additional department maps to be shared with Citizen Additional location based query
Feedback	Live Chat / Phone / Mail Support		
APIs	Custom App development Module	APIs for – - Base maps - Various Query - POI Search	

Enterprise GIS Capability of the Location Engine

Section	Module	Functionality
1	GIS Platform Capability	GIS system should be capable to manage City maps, satellite images, GIS data of various points of interest information, infrastructure and assets etc. of the city. It should provide access to free Online 2D, 3D, Street, Basemap, imagery Services for location reference. GIS system should have a portal for administration that lets administrators to add, update, manage and maintain city GIS data and user management, Content Sharing and capability to build various GIS applications
		GIS data modal should support domains, subtype, spatial rules and relationship, joins and spatial references etc. GIS Solution must have a GIS catalog to manage and maintain the GIS data modal. It must support database administration for user creation and management for GIS database.
		GIS system should have a provision for generation of time bound Geospatial database to enforce export and time restrictions to the GIS database data that is shared with Service providers or other agencies.
		Web GIS system should offer readily available and easy to configure widgets that can be used in making web applications such as base maps, attribute viewer, charts, directions, Draw, Edit, Add data, Geo Processing, Legends, List, Measurement, Scale bar, Search, Incident management, identify Nearby features based on proximity etc.
		Web GIS system should have the capability to change the web pages appearance, and to select services, base maps, templates, galleries and available groups to be used.
		GIS system web GIS application must easily integrate & embed with Microsoft Office application like excel, word etc. for management and city administrators.
		Web GIS should be capable to display legends dynamically on the map that will dynamically change based on the visibility of layers, on zoom in and out.
		Web GIS system should support GIS based dashboards to showcase the results and information in the form of pie charts, bar charts, histograms, threshold bars, query ,highlight and selections etc.
		GIS solution must be commercially off the shelf available that can be configured as per the needs of City utilizing various industry standard best

		practices solutions and templates to reduce the development time.
		GIS solution must support 3D city modelling for urban planning, should support in creation of realistic 3Dcontext and should be able to share these various planning environment on the web as a scene.
		GIS system should support 3D city modelling and should have easy to use desktop editing tools for quick sketching and texturing of 3D building models.
Web GIS Server		
Software	**Functionality**	**Specifications**
2	**Scalability**	The Web GIS server should be highly scalable
		The web GIS server should support following capabilities out of Box (COTS)
		GIS capabilities should be offered by a single software / seamless integration of software based on same technology.
		Web GIS server should support deployment in following cluster environments: Active-Active, Active-Passive.
	Integration & OGC	The software should provide open API & SDKs for developers to build/extend custom web mapping applications. (ex: Qt, .NET, Java, JavaScript).
		Should support Open Geospatial Consortium (OGC) and open web services: including Map, WMS, WFS, WCS, WMTS, WPS, KML and GeoJSON,
		GIS System should support OGC standards like I3S for rendering of 3D data.
		GIS System should support a Service Oriented Architecture (SOA) (GIS on the enterprise service bus).
	Virtualization & Cloud Compatibility	GIS System should support Cloud Environments like Amazon Web Services (AWS) or Microsoft Azure
		GIS System should be capable of deployment on-premises on physical hardware, in a private cloud using VMware or other virtualization technologies, or in the cloud using an Infrastructure as a Service provider (IaaS) such as e.g. Amazon Web Services, Microsoft Azure, IBM Soft Layer, etc.

		The GIS System should support in assessing the platform performance based on benchmark test results against popular physical hardware platforms or virtual server configurations, such as number of platforms per tier and peak server utilization etc. This modules should be regularly updated and should be openly available for the users without additional financial implications.
		GIS System software should support VMware vSphere, Microsoft Hyper-V & Huawei Fusion Sphere virtualization environments.
	GIS Database Management & Editing	GIS System should be capable of maintaining data history, version management and conflict detection.
		GIS System (COTS software) should support database check in – check out / replication functionalities hence maintaining the parent child relationship of Master Database.
		GIS System should support adding data, editing and viewing by multiple users on desktop, web browser and mobile clients.
		Web Editing Application Functionalities like simultaneous Feature editing, isolated editing in separate versions, Undo/Redo operations, snapping by layer, snapping to new geometry, settable snapping, modify, merge, split features, specify an Exact X,Y location, modify and create attribute values, maintain attribute values through defined rules (Domain) etc should be supported by the GIS system.
		The GIS Server software should support Replication across multiple commercial databases in connected and disconnected environments
		GIS Software should support creation of a geographic database, managing geographic database, load spatial data into geographic database.
		GIS system should allow exporting data from the feature service to a file Geospatial Database or SQLite database using custom clients.
		The GIS software should support data relationship such as one-to-many or many-to-many. the rules should allow users to restrict the type of objects in the origin GIS data, table etc. that can be related to a certain kind of object in the destination GIS data, table etc.
	Map Server & Services Management	GIS Server application should record various service statistics, such as total requests, average response time, and timeouts, and reports this information in Server Manager for better monitoring and performance optimization of services.
		GIS Server should have provision to disable publishing new services and blocks most administrative operations during production,
	Supported Environments	The GIS application server and database servers have to be supported on both Windows & Linux platform.

		COTS GIS Server software should support standard Web server / application server like IIS, Apache, Tomcat, Web Sphere, Web logic etc
	Field Applications & SDKs	GIS Server Software ecosystem should have Mobile/apps for Field, Office, community and Application developers.
		The software should have Software development Kit (SDKs) to build and deploy native applications on a variety of popular platforms and devices including Android, Ios, Java, .NET, QT etc.
		The application should provide an out-of-the-box, configurable mobile GIS application on Android, IOS etc, that allows dynamic query and update server data remotely. The mobile application should be able to integrate with external GPS devices.
	Map Visualisation & Spatial Analysis Capabilities	The server should be COTS software and should have the capability to query across multiple map services.
		Should have Centrally managed GIS data, models, tools, maps, and applications
		Should support Tile layer from Vector and Raster layers for better performance and fast accessibility
		Server based GIS should Support any client and device including mobile, smart clients, web browsers (Internet Explorer, Google Chrome and Firefox), geoexplorer applications and desktop applications.
		Server based GIS Software should offer server-based analysis and geoprocessing. This should include vector, scripts, and tools; and synchronous processing.
		Should have out of the box Web Application Functionalities like pan, zoom, identifying features on a map, measure distance, interactive north arrow, magnification window, overview window, find place, query attribute, search attribute, editing, geo-processing tasks, adding base maps etc.
		Should support browser-based access for viewing, editing and analysis of Geo-Spatial Data
		Software should allow character-by-character auto-complete suggestions to be generated as a user types an address in a client application for Geocoding of addresses
		GIS Server Software should support Limited Error Raster Compression for image service caches.
		GIS Server administrator should be able to prevent unauthorized users from accessing cached pages by disabling of caching of service related information by the web browser

		Software should be capable to generate schematic diagrams from the current state of the GIS network data and analyze networks in geographic, schematic, and geoschematic layouts, to meet the utility industry's need to schematically view and manipulate network data.
		GIS software should support Access, create, update, and edit Schematic Diagrams and easily obtain logical views of updated linear network.
		System tools should be able to analyze patterns and aggregate data in the context of both space and time (spatiotemporal) analysis
		The software should have powerful spatial statistics tools for surface modelling using deterministic and geostatistical methods
		The software should support to share 3D services and embed 3D analysis tools
		Should support the OGC I3S standard for cross platform distribution of 3D content for visualization and analysis for field, web, and enterprise application.
		3D layers should capture multiple Levels of Detail (LOD) along with spatial indices, coordinate system information (global, Cartesian, and vertical), and even explicit LOD display information based on screen display parameters.
		Serve geostatistical models for statistically valid prediction services for GIS modeling and visualization.
		COTS Software should support following statistical analysis to predict the values associated with spatial or spatiotemporal phenomena Primarily for environmental sensor reading analysis in order to decide if they pose a threat to environmental or human health and warrant remediation.
		Software should support calculation of empirical semivariogram to explore the spatial relationship
		Software should support Geostatistical interpolation techniques, kriging to utilize the statistical properties of the measured points on a spatial context.
		The techniques should help to quantify the spatial autocorrelation among measured points and account for the spatial configuration of the sample points around the prediction location
		COTS Software should be capable of using following deterministic methods of Geostatistical Analysis to calculate unknown values:
		- inverse distance weighted
		- local polynomial
		- global polynomial

		- radial basis functions
		COTS Software should be capable to make a spatial prediction— From the kriging weights for the measured values, calculate a prediction for the location with the unknown value.
		The COTS software should be capable of accounting the error introduced by estimating the semivariogram model, by using many semivariogram models rather than a single semivariogram.
		COTS Software should be able to identify trends in the cluster of point densities to spatially locate the new, consecutive, intensifying, persistent, diminishing, sporadic, oscillating and historical hot and cold spots based on Getis-Ord Gi statistic P-Value & Z-Score for each feature in a dataset
		Should have geoprocessing framework, geoprocessing tools, core analysis functionalities
	Basemap & Contents	The software provider should host World level free Online 2D, 3D, Street , Basemap, imagery Services
	Security	Server COTS software should support Security, Authentication, and Authorization using
		1. Web-tier authentication (IWA, PKI),
		2. GIS-tier authentication (built-in identity)
		3. Enterprise logins (SAML 2.0),
		4. Enterprise Groups (Active Directory and LDAP) and
		5. TLS 1.0, 1.1, and 1.2
	Database support	Support for Geospatial Databases and Query layers –
		Amazon RDS for Microsoft SQL Server or Amazon RDS for PostgreSQL
		IBM DB2 or Informix
		Microsoft Azure SQL Database or Microsoft SQL Server
		Oracle
		PostgreSQL
		Server Software should support Big Data File Shares like Apache Hadoop HDFS, Apache Hive, Local File Shares (CSV, Shapefile)
		Server Software should support Raster File Share like - AWS S3, Microsoft Azure Storage, Local File Shares
		Server Software should support for Query Layers: ALTIBASE, Dameng, IBM Netezza, SAP HANA, SQLite and Teradata
	Geospatial Bigdata Analytics	Server Software should support On-premise and cloud based Big data analysis of spatial data using Vector & Tabular data
		Server Software should support batch geocode on big tables, CSV files, and Excel files

		Server Software should support to analyse millions of geospatial records on-premise and Cloud to:
		· Aggregate Points based on proximity or administrative boundary
		· Should support Spatial, temporal, and attribute relationships to join features together
		· Reconstruct Tracks based on time stamps captured
		· Software should support to identify overlap between two layers and calculate statistics about the overlap.
		· Based on the criteria specified, Software should support to Find Similar Locations
		· Find Hot Spots tool will determine if there is any statistically significant clustering in the spatial pattern of your data.
		· Software should be able to identify trends in the cluster of point densities to spatially locate the new, consecutive, intensifying, persistent, diminishing, sporadic, oscillating and historical hot and cold spots
		Should be able to perform feature analysis as well as imagery and raster processing using distributed computing with inbuilt tools to analyze patterns, aggregate data in the context of both space/time, extract, process and analyze values from raster imageries etc.
		Server software should support to access the analytical tools via REST API, Python API etc.

Mobile application capabilities

Software	**Functionality**	**Mobile application capabilities**
3	Platform Support	Mobile GIS application should support popular platforms like Android, iOS etc.
		All mobile GIS applications should Interact seamlessly with each other in case of multiple mobile applications.
	Basemap	Mobile GIS application should have access to World level free Online 2D, 3D, Street, Basemap, imagery Services for location reference.
		Mobile GIS application is expected to integrate with enterprise GIS system, which will be the common GIS platform
	Field Workforce Management	Mobile GIS application should support to assign work and Coordinate with field workers
		Mobile GIS application should be capable to report status

		back to the office
	Field GIS data collection	Mobile application should support to Collect and update data in the field, log your current location, and to improve the efficiency of field workforce and the accuracy of your GIS using:
		- Collect and update data using the map or GPS.
		- Connect to feature services (WFS) to edit/update data
		- Download maps to your device and work offline.
		- Collect points, lines, areas, and related data.
		- Fill out easy-to-use, map-driven forms.
		- Attach photos to your features.
		- integrate/ receive data from professional-grade GPS receivers.
		- Search for places and features.
		- Track and report where users have been.
		- Integrate with apps to navigate to location
		- Integrate with apps to assign and monitor status of tasks
	Form based GIS survey capabilities	Mobile application should support to design Surveys with predefined questions that use logic and provide easy-to-fill answers, embedded audio and images, and offer multiple languages.
		Mobile application should support to creation and management of Surveys form /design from a central server over internet.
	GIS Dashboard	Application should monitoring, tracking, and reporting real-time data feeds on maps
		Application should support to create and share operation views that include interactive maps, lists, charts, gauges, and other performance indicators, based on live geographic data defined in a web map or web service. The application should support to configure map views to run on multiple monitors or single-display devices.
	Navigation Capabilities	Mobile application should support to use the data provided or your own data to search the location and navigate directly to the organization's assets
		Application should support voice-guided turn-by-turn directions with automatic route recalculation.
		Navigate completely offline with locally stored data.

		Access navigation data or use your own maps—search your assets, route on your roads, and view your layers.
		Should support use of vehicle-specific travel modes.
		Receive stops from an email, own app, or other ecosystem apps such as apps for field data collection.
MobileApp Development Platform	**Functionality**	**GIS Mobile SDK capability**
4	Platform Support	SDKs should help to build and deploy native applications on a variety of popular platforms like Android, iOS, Java, MacOS, Qt, .NET etc. and for popular devices irrespective of form factor.
	Generic Capabilities	The SDKs should offer development tools to build powerful spatial capabilities to your native apps like GIS analysis, even when offline.
		Developer tools should support to rapidly build GIS-enabled applications with out-of-the-box developer controls.
	Editing Capabilities	Developer tools should support to create and draw graphic features, including points, lines, circles, and polygons, in your application to edit geographic data.
		Developer tools should support to Synchronize edits to feature geometry, attributes, and attachments from a mobile geospatial database to a feature service
		Developer tools should support access to local data and geoprocessing services
		Developer tools should support to enable edit features in mobile geospatial databases, and features in feature services that are public, not secured, accessible on a local network or secured services
	Spatial Analysis	Developer tools should support to perform geographic operations on shapes to create buffers; calculate differences; and find intersections, unions, or inverse intersections of shapes.
	Network Analysis	Developer tools should support to solve and perform network analysis to find the best routes and the closest facilities and determine which routes should be assigned
	3D Analysis	Developer tools should support to effectively visualize and analyze surface in 2D and globe data in three dimensions

4.2 LSCL App (Mobile App):

The Master System Integrator has to integrate and operate the Integrated Mobile app for the various services of Lucknow Municipal Corporation and other departments. Primary objective of this app is to provide information to citizens on various civic services available in the city as well as take feedback from citizens on various services so that the system can be improved. The app shall be available in two modules i.e. for Citizen and Officers Login. Initially the Mobile Application will be hosted on the cloud server and the MSI is expected to closely work with the implementing agency of the LSCL Mobile app for migration of the application and database and hosting to the DC/DR of Lucknow Smart City Limited. The master system integrator has to take over the entire content and database etc of the LSCL Mobile app and migrate the LSCL mobile app to the Data Centre of Lucknow Smart City Limited. The Master System Integrator will operate and maintain the mobile app of Lucknow Smart City Limited throughout the Operation and Maintenance Period.

The Proposed Modules of LSCL Mobile app is detailed below:

Officers App Modules	
❖	Field Work Monitoring Module
❖	GPS Attendance Module
❖	Project Tracking Module
❖	E-Challan Module for unauthorized hawking/encroachment
❖	Alert/Notification
❖	Complaint System
❖	Task Management
❖	Public Toilet Inspection
❖	Parking Inspection
❖	Road Inspection
❖	Dustbin Inspection Module
❖	Task Assignment Module
❖	Citizen Relationship Module (CRM) for Call Center
❖	ICT Based attendance System
❖	GPS Tracking of Vehciles

Citizen App Modules	
❖	About Lucknow Smart City/Lucknow Municipal Coorporation
❖	Zone wise contact details of LMC Staff
❖	My City-My View
❖	My City-My Idea

❖	LMC PGRS
❖	Animal Care
❖	e-complaint
❖	Utilities payment
❖	Advance Booking
❖	Social Media Platform
❖	City Helpline
❖	Traffic Updates
❖	Public Toilets Dashboard
❖	e-Vehicle
❖	e-Hospital
❖	News & Update
❖	Traffic & Parking Availability
❖	Swachh Bharat Mission (Swachhata App)
❖	Property Mutation

4.3 Lucknow Smart City Website:

At present Lucknow Smart City Limited website is hosted at the URL: https://www.lucknowsmartcity.com/ . The Master System Integrator has to take over all the content & database of the already hosted website and host in the Data Centre and Integrate with command and control centre of the Lucknow Smart City Limited. The Master System Integrator has to operate and maintain the website for the period of 5 years. The System Integrator has to implement the Search Engine Optimization and Social Media Optimization for optimum utilization of the website and social media handles of the Lucknow Smart City Limited and will hand over all the contents/database of the Lucknow Smart City Limited on completition of Operation & Maintenance Period at no additional cost.

Scope of Work:

The Master System Integrator shall monitor & optimize Lucknow Smart City websites for performance (e.g. ensuring sites have enough storage space, Website Security, Pages are loading quickly etc.) and ensure adherence to the uptime guarantee, backup frequency and success, etc. Maintenance of all pages, including new pages (English & Hindi) should necessarily be developed and maintained in the CMS. All the new development(s) should be in compliance to existing standards and should be free from all known vulnerabilities and

Bugs. The Master System Integrator has to ensure that modules being developed for the website should go through a mandatory Quality Control and QA testing.

The Master System Integrator has to augment the website of existing Lucknow smart city limited so as to increase the visitor count and will use the various tools and media for maximum citizen engagement through the website. Migration of the website from the old server to the data centre of control and command centre will be under the scope of work for MSI.

Apart from the existing modules of the existing website of Lucknow Smart City Limited, Master System Integrator is supposed to develop the below Modules/attributes on the Lucknow Smart City Website:

S.no	Modules	Attributes
01	**Lucknow City Portal**	Integration with Vahan, Saarthi, Digi-locker, IGRS, PGRS, Shashnadesh, Online Registration System, Swachh Bharat Mission, IT Policy UP, Bhulekh, Disaster Management, e- Suvidha Kendra etc.
		Web Attributes of LSCL Mobile APP- Animal Care, e-complaint system, utilities payment, advance booking, Public Toilets Dashboard, Traffic & Parking Availability etc.
02	**Tourist Centre**	Places of Tourist Interest, Famous Food Joints,
03	**Weather Alert**	Information from Environmental Sensors

MSI has to integrate the various upcoming e-governance/IT initiatives by the various departments on the Lucknow Smart City Websites.

The Master System Integrator is required to perform the following activities but not limited to:-

- **Guidelines**: The MSI should at least comply with the industry standards for website including guidelines, policy framework, security framework proposed by GoI. The security framework of the application is recommended to be based on ISO 27001. The MSI is expected to undertake continuity measures for smooth functioning of the system, risk management plan for the continuity of services, data backup policy and business continuity plan. The entire website should be compliant to cyber security laws & guidelines (http://meity.gov.in/,http://www.cert-in.org.in/ &http://web.guidelines.gov.in/faq.php). The website should adhere the compliance checklist for GIGW guidelines available at http://web.guidelines.gov.in .
- **Preventive Maintenance:** The MSI shall conduct preventive maintenance (including but not limited to inspection, testing, and satisfactory execution of all diagnostics. The selected bidder is required to provide a preventive maintenance checklist along with a schedule.
- Evaluation of suitability/requirement of Servers patches and application of the same on all servers if required.
- **Audit Gap Closure:** The MSI is expected to undertake remedial action for all alerts/audit findings/observations/guidelines raised by the/security system or Government agencies etc. MSI is expected to provide compliance for all LSCL AUDIT observations as and when required and addressing of Audit gaps. The MSI is also expected to extend its support during third party audit, if any, for LSCL website.
- **Content Management System (CMS) & Layout Updates:** Changes to Web Pages, Up- loading / removing / creating /moving of web pages, banners, layout updates, modification/development of graphics-animation, flash content, advertisements etc. Edit, optimize and incorporate content in the form of text, photographs, images and videos etc. provided by LSCL into the website. Providing links to other sites & Urls as and when required. Further development of Special Themes (for National Holidays, Foundation Day etc.) may be required to be developed.
- **Search Engine Optimization:** The MSI shall create SEO Program that results in an increase in overall visitors. Monthly, SEO report must be submitted by MSI. The LSCL website should ranked first in the Search results.

- **Website Security & Performance Monitoring:** The MSI must maintain the integrity of the site against spam, ransom ware, hackers, viruses and electronic attacks via firewalls, security software and passwords and social media postings regarding inappropriate Comments. This would include checking the content given by LSCL itself for in-built vulnerabilities or if they would cause vulnerabilities. An indicative list is provided as below, however the vendor may propose the industry wise best approach ahead :
    - Review various Custom DLL's for potential security breaches.
    - Stop DDoS Attacks
    - Block Phishing Lure Pages
    - Identify DNS & WHOIS Changes
    - Monitor Changes to SSL Certificates
    - Actively Detect & remove Malware and Prevent Intrusions
    - Web performance analysis , Tuning of Database and Operating System
    - Review configurations for OS/IIS provide recommendations
    - Health checks and space utilization.
    - Patch updates
    - Any other GIGW guidelines breaches.
- **Website Monitoring** : Following reports are required to be furnished to LSCL as per the frequency stated:
    - SEO Report (Monthly)
    - Website Performance Report– Google Analytics Report (Monthly)
    - Security Vulnerability Assessment Report (Fortnightly)
    - Ticket Analysis–SLA Response (Weekly, and quarterly compiled report)
- **Help Desk Management**: All Call Log details (website updates / issues etc.) are to be managed and maintained by the MSI. Online access of all Issues/Tickets with as on date status (centralized helpdesk) to be maintained. The knowledge base of issue logs is to be maintained.
- **Security Audit**: At present Lucknow Smart City Website (https://www.lucknowsmartcity.com) has got the security audit certificate from one of the agencies listed at http://www.cert-in.org.in/ . The Master System Integrator has to evaluate the need of security audit before migrating the website and its contents to data centre. If due to any Updation/modifications in the website of Lucknow Smart City Limited there is need for security audit then the MSI has to get the security audit again from anyone of the agencies listed at

http://www.cert-in.org.in/ and the same should be made available to the Lucknow Smart City Website before the publishing of the website in the public domain.

- **Parallel sites:** there should be two (2) sites running parallel, one for testing purposes and the other for production. All maintenance should be carried out in the test environment and be approved before migrating to the live environment.

Below are the minimum Technical & Functional Requirements:

Minimum Functional Requirements	Minimum Technical Requirements

i. Create and manage up-to-date information and content. **ii.** All applications, content, data, and information related to the Online Web- based Portal as well as its users should be securely hosted and saved in the Data Centre. **iii.** Should be light, intuitive, easy to use, responsive, modular, secure, and easy to maintain. **iv.** Should support customization of Look and feel to LSCL/LSCL's requirements. **v.** Website should have an integrated link for the e-governance initiative for G2C services like, IGRS, PGRS, PROPERTY TAX, etc.	**i.** Should be based on Open Standards. **ii.** Should integrate with any other portal products through open standards such as HTML, XML, RSS, web services, and WSRP. **iii.** Should support encryption and compression features **iv.** Shall be OS independent. It must run on Windows, UNIX, Apple and Linux operating systems. **v.** Site must be "responsively designed" to accommodate mobile users. This must include accommodations for slower, cellular internet connections **vi.** Portal must be secure in all the way and all the latest security implementations like https, xss, sql injection, OWASP vunrebelties etc should be implemented/followed to avoid any hacking. **vii.** The portal must be designed for continuous operation, 24 hours a day, 7 days a week with maintenance window clearly defined.

vi. Should be built on industry leading framework and support seamless integration with the backend systems, to easily retrieve and save data. **vii.** Portal must be Omni channel i.e. its design should be such that it can be viewed easily on laptops, tablets and mobiles. **viii.** Should be browser independent and work seamlessly on all leading browsers. **ix.** Should have workflow capabilities with regard to the content approval and publishing process. **x.** Provisions to track and generate web traffic reports for Portal administrators.	**viii.** Shall be browser independent and responsive to run in the same manner on leading browsers like Google Chrome, Mozilla Firefox, Safari, Internet Explorer, etc. **ix.** Shall support Unicode and be multilingual in at least English and Hindi. **x.** Shall have provision for patches, hotfixes and bug fixing solutions. **xi.** Shall adhere to the best possible security standards in the industry. **xii.** Shall support minimum Web 2.0 capabilities **xiii.** Shall be SSL (Secured Socket Layer) compliant and the Developer has to provide appropriate SSL certificate before the portal is made available on public domain. **xiv.** Shall adhere to GIGW, and G.O.I guidelines

5 Common Components

5.1 City Network

Overview

Lucknow is an education and medical hub, trying to take this opportunity Telecom / Internet Service Providers in the city has already laid out fiber covering.

Scope of Work

1. MSI may tie up with an Internet Service Provider or Telecom Service Provider to provide connectivity from the Field Infrastructure to ICCC.
2. The MSI shall prepare the overall network connectivity plan for this project. The plan shall comprise of connectivity of field equipment at the junctions to be connected over network.
3. The actual bandwidth requirement to cater the above mentioned bandwidth parameters and to meet SLAs would be calculated by the MSI and the same shall be clearly proposed in the technical proposal with detail calculations. LSCL also requires the MSI to meet the parameters of video feed quality; security & performance and thus MSIs should factor the same while designing the solution. LSCL reserves its right to ask the Master System Integrator to increase the bandwidth if the provided bandwidth is not sufficient to give the functionality of the system mentioned in the RFP and adhere to the SLAs.
4. MSI should estimate the bandwidth requirement for connectivity between ICCC and Data Center and the same shall be clearly provisioned in the technical proposal with detailed calculations. The connectivity between ICCC and Datacenter shall be through SWAN (State wide area network) or through the existing fiber Network as per the requirement. The bandwidth provisioned needs to adhere to the following minimum benchmark requirements –
    a) Latency should be less than 40 ms
    b) Jitter should be less than 10% of one-way latency
    c) Packet loss should be less than 0.5%
5. The MSI shall meet the parameters of video feed quality, security & performance. MSI should factor the same while designing the solution.

5.2 Data Center and Disaster Recovery:

The authority has decided to host the application and the data of the Integrated Command & Control Centre to the UP State Data Centre (SDC) situated in Lucknow. The Disaster Recovery Centre (DRC) will be the cloud platform developed by the National Informatics Centre. Master System Integrator has to use the state data centre for hosting the application and the

authority will help in necessary documentation for hosting. Tentatively State Data centre will initially provide the below items for the hosting purpose.

- ✓ Rack Space
- ✓ Internet connectivity
- ✓ Physical Security
- ✓ Logical Security
- ✓ Cooling
- ✓ VPN Services
- ✓ WLD Services
- ✓ UPS power
- ✓ Firewall Security

The MSI is expected to consider the above components which will be provided by the State Data Centre.

Data center

- ❖ MSI is required to co-locate all the hardware/software and related items as per the design offered for the smart city infrastructure including SLA monitoring and Help desk management, in a State Data Centre (Tier III+) data Center complying with standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.
- ❖ The Data center shall be available for 24x7x365 operation.
- ❖ The smart city infrastructure shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure.
- ❖ There should be dedicated rack space available in the data center for the entire Smart City project Infrastructure.
- ❖ Access to the Data Center Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel.
- ❖ Racks to be caged.
- ❖ It should have access control system implemented for secured access.
- ❖ Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location

- Physical Access to the building hosting Data Center should be armed and it must be possible to even depute police personnel for physical security of the premises.
- Min 90 days Data Backup of the video feeds and the transaction data for min 1 year shall be stored within the Data Center infrastructure preferable in a cost effective and innovative manner.
- In case the data center services are to go down due to any unforeseen circumstance, the Command Center should have access to the video feeds of previous 90 days and the transaction data for min 1 year from this data backup facility.
- Access logs to be stored for the entire duration of contract and handed over to Authority upon termination/expiry of the contract.

DATA CENTER SPECIFICATION

- Design Standard: Tier-III or above (State Data Centre is Tier III+)
- The availability of data must be guaranteeing to 99.982% availability.
- Receiving Power: Commercial power substation next to DC
- UPS: UPS system with N+N redundancy
- Generator: Gen-set with N+1 redundancy
- Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement
- Cooling Features:
  - ✓ System: Air-cooling system with N+ 2 redundancies, Management of temperature and humidity.
  - ✓ Blow-out Type: Raised flooring air conditioning system, Down-blow below raised floor and drawn into ceiling
- Fire Protection: High Sensitive Smoke Detectors, Fire Suppression System
- **Security:** CCTV surveillance cameras, 24x7 on-site security presence, building Access (Photo Id Card must) along with biometric authentication

Tier 3 DC Min characteristic

i. Tier 3 Data Center Availability: The availability of data from the hardware at a location must be guaranteeing to 99.982% availability.

ii. Redundancy and concurrent maintainability. It requires at least n+1 redundancy as well as concurrent maintainability for all power and cooling components and

distribution systems. Any such component's lack of availability due to failure (or maintenance) should not affect the infrastructure's normal functioning.

iii. No more than 1.6 hours of downtime per year

iv. N+1 fault tolerant providing at least 72 hour power outage protection

v. All IT equipment is dual-powered and fully compatible within the topology of a site's architecture.

The Data center shall primarily be divided into two zones:

A. Server Infrastructure Zone

This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data center LAN connections shall be provided through switches placed in this area. Access to this zone, where the surveillance project IT infrastructure is hosted, shall be demarcated and physical access to the place shall be given only to the authorized personnel. Indoor CCTV Cameras shall be installed to monitor the physical access of the system from remote location.

B. UPS and Electrical Zone

This zone shall house all the Un-Interrupted Power Supply units, Main Power Distribution Units (PDUs) to feed the components such as PAC, UPS, lighting, fixtures etc. This shall also house all the batteries accompanying the UPS components. As these generate good amount of radiation, it is advised to house these components in a room separate from server infrastructure zone.

IT Infrastructure for Data center

Following sections highlight the indicative scope of work of the MSI and not limited for Design, Supply and Deployment of IT Infrastructure for Data center

1) **Hardware and Network Provisioning** :MSI shall be responsible for the following but not limited to:

- ✓ Appropriate sizing and provisioning of IT infrastructure like servers/storage, network devices (like routers/switches etc.), security equipment including firewalls, etc. with the required components/modules considering redundancy and load balancing in line with minimum technical requirements
- ✓ Warranty for all the IT hardware assets procured to comply with the requirements as defined in this RFP.
- ✓ Size the bandwidth requirements across all locations considering the application performance, replication, data transfer, internet connectivity for Data center and other requirements.
- ✓ Furnish a schedule of delivery of all IT Infrastructure items.
- ✓ Ensure all the hardware requirements of the application suite (including third party applications), databases, OS and other software are met.
- ✓ Authority may at its sole discretion evaluate the hardware sizing. The SI needs to provide necessary explanation for sizing to Authority
- ✓ Ensure that the proposed servers are able to accommodate newer versions of processors, memory, etc. that support enhanced capability (e.g. lower power footprint, higher working temperature, smaller process architecture, higher frequency) of operation if required, whenever they are available. To further clarify, motherboard, controllers, etc. provided shall be of latest architecture available that supports such newer version. MSI shall substantiate with proof; preferably with an undertaking to replace the processors as and when such processors of highest level of frequency are supported.
- ✓ The proposed server models wherever applicable shall be Blade Mount servers with key board, monitor, etc. shared to minimize the requirement of rack space in Data center considering any space constraints. The model however shall not pose constraints in performance.

2) Provisioning switches

- ✓ The MSI shall size and propose requisite switch at Data center with the required components/modules considering redundancy and load balancing.
- ✓ The MSI shall size and propose other switches required for interconnecting various segments, operations center, work area, etc.

3) IP address schema

- ✓ The MSI shall design suitable IP Schema for the entire Wide Area Network including Data center and interfaces to external systems/network. The MSI shall ensure efficient traffic routing irrespective of link medium.
- ✓ The MSI shall maintain the IP Schema with required modifications from time to time during the project period.
- ✓ MSI should provide the unique identity schema similar to addressing schema for all hardware components.

4) Sub-Networks & Management of Network operation

- ✓ The proposed architecture of Data center shall be divided into different sub-networks. These networks shall be separated from other networks through switches and firewalls. The logical separations of these sub-networks shall be done using VLANS.

- ✓ A separate VLAN shall be created to manage the entire network. This network shall have systems to monitor, manage routers, switches, Firewalls, etc. The SI shall provide necessary hardware / server for loading the monitoring software if required.

5) Provisioning Storage

- ✓ Storage requirements for the application suite shall have to be assessed by the SI and the storage solution shall be sized and procured accordingly. SI shall propose appropriate storage mechanism in order to accommodate proposed application suite requirement of the Authority
- ✓ The proposed storage shall be configured with appropriate redundancy to maintain business continuity

6) Network Equipment level redundancy

- ✓ The MSI shall provide real-time redundancy at the network equipment level in Data center, and there shall not be any single point of failure.
- ✓ All equipment shall be provided with dual power supply modules. Each of the two supply modules shall be connected to alternate power strips of the network rack (two power strips to be provided in each network rack).
- ✓ The Network Equipment redundancy stipulations wherever prescribed are the minimum requirements that the MSI needs to consider. However, SI needs to estimate and plan actual requirements considering service level requirements specified in this RFP.

7) Provisioning IT Security Equipment

- ✓ The MSI shall size and propose firewalls with the required components/modules for ICCC/Data center.
- ✓ Necessary IDS/ IPS shall be provided for monitoring the traffic of all the VLANs at Data center/ICCC.
- ✓ Necessary devices for log capture from servers, network equipment and other devices shall to be provisioned.
- ✓ The MSI shall implement DNS server so that the URL can be used instead of accessing web server using IP address directly.
- ✓ MSI shall implement management systems and procedures that adhere to Authority's security policies.
- ✓ MSI shall secure network resources against unauthorized access from internal or external sources.
- ✓ MSI shall also provide a mechanism for tracking security incidents and identifying patterns, if any. The tracking mechanism shall, at a minimum, track the number of security incident occurrences resulting in a user losing data, loss of data integrity, denial of service, loss of confidentiality or any incident that renders the user unproductive for a period of time
- ✓ MSI shall ensure that all firewall devices are staged and comprehensively tested prior to deployment. In addition, SI shall conduct a vulnerability scan and analysis of the network to ensure that the optimal policies are instituted on the firewall.
- ✓ MSI shall ensure that all firewall management is initiated from a segregated management rail on the network.
- ✓ MSI shall provide intrusion management services to protect Authority's resources from internal and external threats.
- ✓ MSI shall provide Authority with the necessary hardware/software required for efficient intrusion management.
- ✓

Disaster Recovery (DR) Site

- Disaster Recovery Site will be on Meghraj cloud platform (National Informatics Centre) with 100% uptime. The bidder has to work on requirement of server configuration, Web Server, OS Platform, Environment as per the requirement of the project. The authority will help in necessary documentation with National Informatics Centre for Hosting. The MSI is

required to provision for a Disaster Recovery (DR) Site same as of main Data Center (DC) capacity & standard for Smart City Solution. The DR site should not be in the same seismic zone and should be at least 250 km from Main DC site. DR site shall provision to cater to 100% load of the smart city system. There shall be no loss of video recording in case of failure of any single server and storage component. Both DC and DR Site shall work in an Active-Active mode with 100% recording of cameras and application availability of all smart city components. The MSI shall establish dedicated connectivity between the DC and DR Site for replication & failover. The MSI shall submit the detailed solution document for the DR Site solution with justification for the proposed design meeting the requirements. Authority would carry out a detail assessment of the proposed location for the Smart City Disaster Recovery Center on the parameters of Safety & Security and reserves it right to accept or reject the proposed site for Disaster Recovery center. In case the proposed site is not acceptable to Authority, Successful Bidder shall suggest alternatives matching the requirements mentioned above. Authority may also ask the respective bidder to arrange for a visit during bid evaluation stage. Both DC and DR site shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure. There shall be no loss of video recording in a CCC in case of failure of any single server and storage component.

Both DC and DR Site shall work in an Active-Active mode. The SI shall establish dedicated connectivity between DC and DR Site for replication & failover. The SI shall design the DC and DR solution with the necessary load balancing, replication and recovery solution that provide zero RPO (Recovery Point Objective) and RTO (Recovery Time Objective) of 10 minutes. The DC and DR site shall be periodically audited; updated and mock drills shall be performed. Along with the findings and improvement /corrective steps to be taken to concerned authority the bidder shall submit the detailed solution document for Dc and DR Site solution with justification for the proposed design meeting the requirements alongwith the bid.

DC/DRC Monitoring Dashboard

❖	MSI should provide a dashboard view for their DC/DRC solution for LSCL for virtually monitoring all smart city projects related DC & DRC activities inclusive of hardware, application, data, bandwidth, manage hosting services, storage from the ICCC.
❖	The system should provide ability to monitor, manage, control and report performance of all smart city project servers.
❖	The system should have virtual server dashboard to monitor and manage capacity of server, utilization, devices and services running on server.
❖	The system should allow for easy deployment of servers, operating systems application and services for integrating and managing such components collectively.
❖	The system should provide rack-view monitoring for power consumption, capacity, services deployed, and servers up, down and in critical state.
❖	The system should provide browser and OS independent console and web interface.
❖	The system should automatically act on policy deployment, pre- configurations and pre-defined SOPs.
❖	The system should provide route cause analysis in case of failure.
❖	The system should automatically log incidents and generate real-time alerts.
❖	The system should stringent role based security model to allow any authorised users to access and administer the system.
❖	The system should able to generate automatic and manual notifications, alerts and reports based on performance to the concerned operators/individuals.
EMS with Helpdesk	

❖	For effective operations and management of IT Operations, there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: a) Network Fault Management b) Network Performance Management c) Network Flow Traffic Monitoring d) Application Performance Management e) Server Performance Monitoring f) Centralized Log Management g) Centralized and Unified Dashboard h) Centralized and Customizable Service Level Reporting I) Help Desk for Incident Management The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: • Event and Alarm management, • Auto-discovery of the IT environment, • Performance and availability management • Correlation and root cause analysis • Service Level Management, notifications • Reporting and analytics • Automation and Customization
❖	There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.
❖	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.
❖	The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue.
❖	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events
❖	Scalability – The system should be capable of supporting at least 100 thousand network flow per second on single server with capability to capture each unique traffic conversations

❖	Scalability – The solution must be scalable, it should be able to support upto 25000 log events per second and also be able to support beyond 25000 EPS by Linearly adding more servers of either reference system type, depending on the size of the expected load.
❖	The solution shall provide future scalability of the whole system without major architectural changes.
❖	The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.
❖	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
❖	The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components
❖	Consolidated dashboard of the proposed EMS solution must be able to do dynamic service modelling of all business critical production services & use near-real time Service Model for efficient cross domain topology based event correlation.
DETAILED Minimum SPECIFICATIONS: EMS	
Consolidated Dashboard	
❖	The platform must provide complete cross-domain visibility of IT infrastructure issues
❖	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc.
❖	The solution should support dynamic discovery to maintains Run-time Service Model accuracy e.g. virtualization and cloud
❖	The solution must support custom dashboards for different role users such as Management, admin and report users
❖	The solution must allow creating custom data widget to visualize data with user preferences
❖	The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.
❖	The proposed solution must support capacity views to find most consumed resources.
❖	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console
❖	The solution should allow for customizable operator perspectives
Network Performance Management:	
❖	The proposed solution platform shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.

❖	The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the- box implementation automating the work required to use validated designs and best practices.
❖	The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
❖	The proposed solution must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different colour depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used.
❖	The proposed solution must have suitable system level backup mechanism for taking backup of NM data manually of at least one month.
❖	The proposed solution must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc.
❖	The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month, 6 months etc alongwith the current status.
❖	The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status
❖	The proposed solution must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.
❖	The proposed solution should have multiple alerting feature to get the notification via email, sms and third party systems
❖	The proposed solution must support listening to traps and syslog events from the network devices with retention period upto 6 months.
❖	The proposed solution must support defining the data retention period to control storage
❖	The solution must support custom device template to support Generic SNMP devices
❖	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
❖	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.

System and Application Monitoring:	
❖	The solution should offer service driven operations management of the IT environment to manage distributed, heterogeneous systems - Windows, UNIX & LINUX from a single management station.
❖	The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms Or events to point out the probable cause using remedy actions - E.g. pull the top 5 processes consuming most of the CPU when CPU alarm triggers
❖	The solution should provide a centralized point of control with out-of-the-box policy-based management intelligence for easy deployment for the servers, operating systems, applications and services for correlating and managing all the IT infrastructure components of a business service
❖	The solution shall be able to monitor Hypervisor host hardware status e.g. fans, disk, memory, CPU etc.
❖	The solution must support SNMP v1-3, PowerShell, SSH, JDBC, HTTP, JMX, collected agents for monitoring various type of devices and systems
❖	It should also be able to monitor various operating system parameters depending on the operating system being monitored and setting thresholds.
❖	The solution should support Virtual platforms - VMware and Microsoft Hyper-V, Citrix Xen, AWS, Azure and provide capability to monitor both Microsoft .NET and J2EE applications from the same platform
❖	The solution should provide support for maintenance window and scheduled downtimes
❖	The solution should measure the end users' experiences based on transactions without the need to install agents on user desktops.
❖	The solution must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.
❖	The solution must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.
❖	Solution shall be able to monitor customer transaction by end-user name, and thus able to understand exactly which customers were impacted, their location, type of browser used etc.
❖	The solution must simplify complex app topologies through task–relevant views based on attributes such as location, business unit, application component etc.
❖	The solution must proactively monitor 100% of real user transactions; detect failed transactions; gather problems that affect user experiences and prevent completion of critical business processes.

❖	The solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view.
❖	The solution must provide proactive real-time insights into real user behavior, trends, log analytics and performance to enhance customer experience across various channels
Fault Management:-	
❖	The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
❖	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: • Event filtering • Event Deduplication • Event aggregation • Event masking
❖	The proposed solution must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures.
❖	The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.
❖	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.
❖	Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream based correlation should be made available.
❖	The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event
❖	The proposed monitoring solution should have capability to configure actions based rules for set of pre-defined alarms/alerts enabling automation of set tasks.
❖	The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management
❖	The solution should classify events based on business impact

❖	The solution should allow creation of correlation or analytics rules for administrators
❖	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms
Log Management:-	
❖	The proposed solution must provide a common classification of event irrespective of the log format
❖	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes.
❖	The log data generated should be stored in a centralized server. The period upto which the data must be available should be customizable.
❖	The proposed solution must support logs collected from commercial and proprietary applications i.e. Microsoft, Cisco, Brocade, HP, Security System, Firewall, Access Points etc.
❖	The proposed solution must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server etc. using agents
❖	The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.
❖	The system shall support the following log formats for log collection : o Windows Event Log o Syslog o Access Log Data o Application Log data o Any Custom Log data o Text Log (flat file)
❖	The solution should be able to collect raw logs in real-time to a Central log database from any IP device including: • Networking devices(router/switches/voice gateways) • Security devices (IDS/IPS, AV, Patch Mgmt., Firewall/DB Security solutions) • Operating systems(Windows 2003/2008,Unix,linux,AIX) • Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere 4.X, vDirector, Citrix) • Databases(Oracle/SQL/MYSQL/DB2)
❖	The collection devices should support collection of logs through Syslog, syslog and also provide native Windows Agents as well as Agentless(PowerShell) connectors
❖	The proposed solution must provide alerting based upon established policy

❖	The proposed solution must provide SDK/API to write custom connectors and collectors to pull log and monitoring data from third party system
❖	The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.
❖	The proposed solution must collect, index the log messages and support full-text searching for forensic investigation
❖	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
❖	The solution must provide pre-defined log correlation rules to detect suspicious behavior
❖	The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern
❖	The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose
❖	The system shall have the capability to drag and drop building of custom queries & reports.
❖	The system shall be capable of operating at a sustained 10000 EPS per collection device. The system shall provide the ability to scale to higher event rates by adding multiple collection devices.
Network Flow-based Traffic Analysis	
❖	The proposed traffic monitoring system must be able to track all flow of traffic on the network and identify malicious behavior with all IP conversations.
❖	The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.
❖	The proposed system must provide eight-hour, daily, weekly, monthly, yearly, or customizable reporting time periods.
❖	The proposed solution must be able to monitor and report on a variety of unique protocols (used in the overall deployed solutions) per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.
❖	The proposed solution must keep historical rate and ip to ip, ip to protocol, protocol to protocol conversation data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.
❖	The proposed solution must keep historical rate and protocol data for a minimum of 60 days (most recent) in its short term operating database. All data in that database must have a maximum 1 minute window granularity.
❖	Flow collection systems must support a minimum of 6 million flows per minute and be capable of storing gathered information in a common database where all long term reporting information is held.

❖	• The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions. • Search for any traffic using a specific configurable destination port, or port range. • Search for any protocol in use by a specific host, interface or list of hosts or interfaces.
	Helpdesk - Incident Management
❖	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface
❖	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
❖	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
❖	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
❖	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties
❖	The proposed solution should automatically suggest available technicians based on workload while assigning tickets
❖	The proposed solution should tightly integrate with monitoring system to provide two way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts
❖	The proposed system must not create more than ticket for same recurring alarm to avoid ticket flooding from Monitoring system
❖	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web based console with no programming
❖	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email
❖	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team

❖	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
❖	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues
❖	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type
❖	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
❖	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window
❖	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.
❖	The proposed solution allow scheduling periodic report to check current software and hardware inventory
	Service Level Reporting:
❖	The solution must provide Out of the box reporting templates for performance, availability, operation, virtualization and capacity and audit
❖	The solution should provide reports that can prove IT service quality levels, such as application response times and server resource consumption
❖	The system reports should be accessible via web browser and Reports can be published in PDF and csv format
❖	The solution must provide Reports that can be scheduled to publish automatically or they can be produced on demand
❖	The solution should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels
❖	The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components. The solution should provide correlation between Network, Server and Application to identify the business impact from the specific event or alarm
❖	The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.
❖	The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.
	Role-Based access control:-
❖	The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department

❖	The Solution should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.
EMS Other Key Requirements:-	
❖	The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
❖	The solution should be deployable on Linux operating systems to reduce the overall TCO
❖	The solution should run without any propriety database license for data store - Data store must be bundled within EMS (E.g. popular time-series, no-sql, HBase based monitoring systems) to reduce the TCO
❖	The solution must provide way to define key performance indicators (KPIs) within the Business Service Management module.

Technical Requirement

WAN / Internet Router	
❖	Multi-Services: Should deliver multiple IP services over a flexible combination of interfaces
❖	Ports: As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
❖	Interface modules: Must support up to 10G interfaces as per the design. Must have capability to connect with variety of interfaces.
❖	Protocol Support : • Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC • Must support VPN • Must have support for integration of data and voice services • Routing protocols of RIP, OSPF, and BGP. • Support IPV4, IPV6 • Support load balancing
❖	Manageability: Must be SNMP manageable
❖	Traffic control: Traffic Control and Filtering features for flexible user control policies
❖	Bandwidth: Bandwidth on demand for cost effective connection performance enhancement

❖	Remote Access: Shall have remote access features
❖	Redundancy: • Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis • All external interface modules, power supplies should be hot- swappable
❖	Security features: • MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS/AAA Authentication • Management Access policy • IPsec / Encryption • L2TP
❖	QOS Features: • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy Bandwidth Reservation / Committed Information Rate

Data Centre TOR (Top of the Rack) Switch	
❖	Ports: • 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra 2 numbers of Uplink ports (40GE) • All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports.
❖	Switch type: Layer 3
❖	MAC: Support 32K MAC address.
❖	Backplane: Capable of providing wire-speed switching
❖	Throughput: 500 Mpps or better

❖	Port Features: Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
❖	Flow Control: Support IEEE 802.3x flow control for full-duplex mode ports.
❖	Protocols: • IPV4, IPV6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring • DHCP support • Support up to 1024 VLANs • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection • Should support Ring protection
❖	Access Control: • Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication
❖	VLAN: • Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent
❖	Protocol and Traffic: • Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number

❖	Management: • Switch needs to have a console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface.
❖	Resiliency: • Dual load sharing AC and DC power supplies • Redundant variable-speed fans
Servers	
❖	Processor: • Latest series/ generation of 64 bit x86 processor(s) with Ten or higher Cores • Processor speed should be minimum 2.4 GHz • Minimum 2 processors per each physical server
❖	RAM: • Minimum 64 GB Memory per physical server
❖	Internal Storage: • 2 x 300 GB SAS (10k rpm) hot swap disk with extensible bays
❖	Network interface: • 2 X 20GbE LAN ports for providing Ethernet connectivity • Optional: 1 X Dual-port 16Gbps FC HBA for providing FC connectivity
❖	Power supply: • Dual Redundant Power Supply
❖	RAID support: • As per requirement/solution
❖	Operating System: • Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system)
❖	Form Factor: • Rack mountable/ Blade

❖	Virtualization: • Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE and Citrix.
Blade Chassis Specifications	
❖	Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades
❖	Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided
❖	Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.
❖	Have the capability for installing industry standard flavours of Microsoft Windows, and Enterprise Red Hat Linux Oss as well as virtualization solution such as VMware.
❖	DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades allowing remote installation of software
❖	Minimum 1 USB port
❖	Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with
❖	Two hot-plugs/hot-swap redundant 16 Gbps Fibre Channel module for connectivity to the external Fibre channel Switch and ultimately to the storage device
❖	Hot plug/hot-swap redundant power supplies to be provided, along with power cables
❖	Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.
❖	Required number of PDUs and power cables, to connect all blades, Chassis to Data Centre power outlet.
❖	Hot pluggable/hot-swappable redundant cooling unit
❖	Provision of systems management and deployment tools to aid in blade server configuration and OS deployment
❖	Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.
❖	Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP
❖	Dedicated management network port shall have separate path for remote management.
Primary Storage	

❖	Solution/ Type: IP Based/iSCSI/FC/NFS/CIFS
❖	Storage: • Storage Capacity should be minimum 5 TB (usable, after configuring in offered RAID configuration) • RAID solution offered must protect against double disc failure. • Disks should be preferably minimum of 3 TB capacity • To store all types of data (Data, Voice, Images, Video, etc.) • Storage system capable of scaling vertically and horizontally
❖	Hardware Platform: • Rack mounted form-factor • Modular design to support controllers and disk drives expansion
❖	Controllers: • At least 2 Controllers in active/active mode • The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
❖	RAID support: • RAID 0, 1, 1+0, 5+0 and 6
❖	Cache: • Minimum 128 GB of useable cache across all controllers. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.
❖	Redundancy and High Availability: • The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies

❖	Management software: All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. • Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, up to max capacity of the existing controller/units. • A single command console for entire storage system. • Should also include storage performance monitoring and management software • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures • Should be able to take "snapshots" of the stored data to another logical drive for backup purpose
❖	Data Protection: The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours.

Secondary Storage	
❖	Solution/Type: • Secondary Storage (Archival/Backup) can be on any media such as Tapes, Disks, Disk systems, etc. or its combination. (so as to arrive at lower cost per TB) • May or may not use de-duplication technology • Compatible with primary storage • Must use latest stable technology platform, with support available for next 7 to 10 years.
❖	Backup Size: • To store data as required, to meet the archival requirement for different type of data/information
❖	Hardware Platform: • Rack mounted, • Rack based Expansion shelves

❖	Software Platform: • Must include backup/archive application portfolio required
❖	Retrieval time: • Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data. This would be taken into account for SLA calculation. (Critical data means any data needing urgent attention by the Judicial System or by Police Dept. for investigation / terrorist treat perception).

KVM Switch	
❖	KVM Requirement: Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre
❖	Form Factor: 19” rack mountable
❖	Ports: minimum 8 ports
❖	Server Connections: USB or KVM over IP.
❖	Auto-Scan: It should be capable to auto scan servers
❖	Rack Access: It should support local user port for rack access
❖	SNMP: The KVM switch should be SNMP enabled. It should be operable from remote locations
❖	OS Support: It should support multiple operating system
❖	Power Supply: It should have dual power with failover and built-in surge protection
❖	Multi-User support: It should support multi-user access and collaboration
Server Load balancer	
❖	Server Load Balancing Mechanism: • Cyclic, Hash, Least numbers of users • Weighted Cyclic, Least Amount of Traffic • NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
❖	Redundancy Features: • Supports Active-Active and Active-Standby Redundancy • Segmentation / Virtualization support along with resource allocation per segment, dedicated access control for each segment

❖	Routing Features: • Routing protocols RIPv1/RIPv2/OSPF • Static Routing policy support
❖	Server Load Balancing Features: • Server and Client process coexist • UDP Stateless • Service Failover • Backup/Overflow • Direct Server Return • Client NAT • Port Multiplexing-Virtual Ports to Real Ports Mapping • DNS Load Balancing
❖	Load Balancing Applications: • Application/ Web Server, MMS, RTSP, Streaming Media • DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH, LDAP, RADIUS
❖	Browser Type Farm: • Support for Global Server Load Balancing • Global Server Load Balancing Algorithms • HTTP Redirection, • HTTP • DNS Redirection, RTSP Redirection • DNS Fallback Redirection, HTTP Layer 7 Redirection
❖	URL based SLB
❖	Http header super farm
❖	SLB should support below Management options • Secure Web Based Management • SSH • SNMP v1, 2, 3 Based GUI • Command Line
Tape library	
❖	Make: Must be specified by MSI
❖	Model: Must be specified by MSI. All relevant technical information/brochures must be submitted
❖	Technology: LTO 6
❖	Number Drives: Two LTO 6 Drives

❖	Media Slots: Minimum 45
❖	Interface: Minimum 4 Gbps FC Interface
❖	Power Supplies :Redundant Hot Swap Power supply
❖	Fans: Redundant Hot Swap cooling fans
❖	Software: Security and Remote Management Software
❖	Supported Backup Software: Should support industry leading backup software such as Symantec Net Backup
❖	Accessories: With all required cables and accessories to install and configure in standard 19" rack and to connect to Server/SAN switch
Link Load Balancer	
❖	Link load balancer shall be an appliance based solution with minimum 64 bit speed core architecture and purpose built hardware for overall high performance. It shall have a minimum of 64 GB RAM and at least 8x10G SFP+ ports. It shall have minimum of 120 Gbps throughput. Shall support security features like reverse-proxy firewall, sync-flood and denial of service attack protection from day one. It shall support multiple Internet links in active-active load balancing and active-standby failover mode.
❖	It shall support built-in failover decision/health-check conditions. It shall also support failover and High Availability (HA) requirements. It shall have redundant power supplies. Shall support script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS.
Server Load Balancer	
❖	Multi-tenant hardware with multicore CPU support. It shall support minimum four (4) virtual instances and shall be scalable to 16 instances on the same appliance. Shall have minimum of 10 Gbps of system throughput per virtual instance to support multiple load balancing and security functions. Shall have minimum of 8x10G SFP+ interfaces from day one. Shall have security features like reverse-proxy firewall, sync-flood and denial of service attack protection from day one.
❖	Server load balancers shall support script based functions support for content inspection, traffic matching, and monitoring of HTTP, SOAP, XML, diameter, generic TCP and TCPS.

Databases

Any commercially available database shall be provided along with license and support and upgrade costs.

Functional Requirements

Databases	
❖	Database License should be un-restricted and perpetual, to prevent any non-compliance in an event of customization & integration.
❖	Databases shall support multi hardware platform.
❖	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
❖	Database shall have built-in backup and recovery tool, which can support the online backup.
❖	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.
❖	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single database/multiple database.
❖	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
❖	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
❖	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real-time reports from the DR site without stopping the recovery mechanism.
❖	Database shall have Active-Passive failover clustering with objectives of scalability and high availability.
❖	Database shall provide mechanism to recover rows, tables when accidentally deleted. The mechanism should provide ways and means of recovering the database.
❖	Database shall provide functionality to replicate / propagate the data across different databases.
❖	Ability to add nodes to cluster on fly with no downtime with-out Unloading/ reloading data.
❖	The RDBMS should support partitioning feature in table level object.
❖	Database shall provide native functionality to store XML, Images, Text, Medical Images, CAD images etc within the database and support search, query functionalities.
❖	Database shall include tools for enterprise class high availability solution like monitoring performance, diagnose and alert for problems, tuning bottlenecks, resource monitoring and automatic resource allocation capabilities.

❖	RDBMS must support the SQL queries.
❖	Database shall provide security mechanism at foundation level of the database, so that the options and additions to the database confirm the security policy of the organization without changing the application code. Shall confirm to security evaluations and conformance to common criteria.
❖	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
❖	Database shall support for enhanced authentication by integrating tokens and biometric technologies.
❖	Database shall provide functionality for classifying data and mediating access to data based on its classification for multi-level security and mandatory access control, manage access to data on a "need to know" basis.
❖	Database shall be having native auditing capabilities for the database. Should support optional Audit Capability to store the audit records in separate audit store with monitoring & reporting for multiple databases to detect any security breaches.
❖	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
❖	The Management tool should provide advisory-based performance tuning tool which help to tune the queries or objects, SQL analysis, SQL access.
❖	The enterprise database should provide single web-based console for management of the database.
Restart and Recovery	
❖	Availability of recovery/restart facilities of the DBMS.
❖	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
❖	Program restart should be provided from the point of failure.
❖	Ability to manage recovery/restart facilities to reduce system overhead.
❖	Provides extra utilities to back up the databases by faster means than record by record retrieval.
❖	Provides clear error reporting, recovery and logging.
❖	Describe recovery strategies that need to be in place.
❖	System should support mirroring for DRP.
Backup Procedures	
❖	Describe Backup Procedures you plan to deploy.

❖	Describe backup application(s) your proposed solution use.
❖	Provide details of data backup and restore processes and procedures for all data elements.
❖	Provide details of automated archiving procedures to copy active data to storage media when archive 'age' is reached.
Error Handling	
❖	Ability to trap a transaction failure through: • Application Software • DBMS • Availability of manual containing all system error messages and correction procedures
System Control	
❖	Provide details of the 'Audit trail' facility for your proposed solution.
❖	Should provide adequate auditing trail facility.
❖	System should record the date and time stamp for all records.
❖	Ability to track terminals from where the system is accessed.

Functional Requirements

Communications Cabinets with Racks	
❖	The cabinets shall be capable of accommodating all the network devices to support the design requirements.
❖	All cabinets shall be designed to carry the anticipated load of all equipment that shall be installed inside the cabinet including having at least 30% spare capacity per rack.
❖	All cabinets shall be provided with standard accessories including vertical and horizontal cable manager, lights, fans, and power bars as needed to support the design requirements of this Project.

Technical Requirements

Communications Cabinets with Racks	
❖	The cabinets shall be capable of accommodating all the network devices to support the design requirements and shall include at least size 42U racks.

❖	All cabinets shall be supplied with standard 19" wide rack mount assemblies that shall allow for mounting of standard rack-mount equipment.
❖	All cabinets shall be supplied with standard lockable doors.
❖	The cabinets shall be IP55 rated.
❖	All cabinets shall have provision for cable entry from top & bottom of rack with knock-off, pre-punched marked openings.
❖	All cabinets shall have vertical cable managers in front with suitable accessories on each side of the rack with covers for concealed wiring within the rack.
❖	Front door shall be made of Tinted toughened glass and should be lockable.
❖	All cabinets shall have equipment mounting frame (rail notches) for mounting of equipment.
❖	Shelves for equipment placement shall be provided as required.
❖	All cabinets shall be designed to carry the anticipated load of all equipment that shall be installed inside the cabinet with at least
❖	All cabinets shall be provided with standard accessories including vertical and horizontal cable manager, lights, fans, and power bars as needed to support the design requirements of this Project.
❖	The rack shall have ventilation louvers or uniform perforations on side panel & rear door & equipment cooling with fans (4nos.) housed in fan trays.
❖	Two strips each with minimum 8 numbers of 5A/15A, 230 VAC power outlets with MCB, inbuilt surge suppressor & line filter for conditioned power output shall be provided.
❖	The device shall support operating temperature range of 0°C to +45°C with ambient relative humidity of 10-90% non-condensing.
Outdoor Enclosure (as needed)	
❖	Minimum 6RU weather proof NEMA 4X/IP65 compliant UV resistant outdoor metallic enclosure in conformance with DIN
❖	Vandal proof design with single side door and with minimum IP 55 compliant industrial lock.

5.3 Data Security

The smart city network architecture shall adopt an end-to-end security model that protects data and infrastructure from malicious attacks, thefts, natural disasters, etc. The architecture shall be implemented in such a way that the system is protected from hackers and other threats. The data security system shall address security policies, hardware and software, along

with the connectivity between the field device and the respective application. Note that the client at its discretion may have the authority to carry a security audit of the entire system during the course of the Project or post implementation at regular intervals.

Functional Requirements & Technical Requirements of Security Component	
❖	An end-to-end data security system shall be provided for strong and reliable security for the entire infrastructure, active electronics, Wi-Fi system, surveillance system, and other field equipment, software and hardware.
❖	Overall, the IT architecture shall refer to the architecture suggested by National Institute of Standards and Technology (NIST) and CSA's (Cloud Security Alliance) Cyber Security Guidelines for Smart City Technology Adoption.
❖	MSI should ensure the compliance of Cyber Security Model Framework for Smart Cities released by Ministry of Urban & Development vides his OM no: K-15016/61/2016-SC-1 dated 19th May 2016/released by National Security Council, Secretariat, and Government of India.
❖	Firewall shall be implemented at ICCC and at DC/DR as per the site requirement.
❖	Security services used to protect the overall solution shall include: identification, authentication, access control, administration and audit, as per industry standards and protocols.
❖	System shall support advanced user authentication mechanisms including digital/e-certificates, biometric authentication, e-signatures, etc. and shall have compliance with all state level and national level initiatives.
❖	Security design shall support industry standards based identity management system, security of physical and digital assets, data and network security, backup and recovery, along with disaster recovery system.
❖	The system shall be capable of detecting denial of service (DDoS) and remediation.
❖	The system shall include industry standards based firewall and antivirus, and shall provide content filtering, tracking, lockdown, and malware detection and prevention capabilities.
❖	The MSI shall ensure that the security policy is maintained and updated as per the latest industry standards including ISO 27001, BS 7799 and BS 15000 guidelines.

❖	Message exchange between various applications should be fully encrypted and authenticated. Any applications hosted on cloud should talk to the applications hosted on cloud only through predefined APIs.
❖	All applications hosted on cloud should support multi-tenancy with adequate authentication, encryption and role based access control mechanism.
❖	All communications to the devices and their respective management applications shall happen through the Project specific network. Adequate security checks to protect the data shall be implemented as part of the overall data security.
❖	Any wireless sensors implemented as part of the Project shall only communicate to authorized wireless networks and shall not connect to rogue networks. This shall be in compliance with the guidelines as published by Ministry of Communications & Information Technology.
❖	Wireless layer of the network shall be segmented for public use and for city utilities by using VPN or separate networks in the wired core.
❖	All traffic from city equipment/sensors to the application servers shall be encrypted Secure Socket Layer (SSL) or SSH and authenticated prior to sending any information. The data at rest or in transmit must be encrypted.
❖	All authentication of sensors in the network shall happen at the time of implementing the sensors and adding them to the system and shall be based on physical characteristics of sensors like MAC ID, Device ID, etc.
❖	The field equipment shall not have any physical interface for administration. Monitoring of systems and networks shall be undertaken remotely.
❖	The ICCC facilities shall have the following – firewall, intrusion detection and intrusion prevention systems, web application firewalls, behavioral analysis systems for anomaly detection, correlation engine, denial of service prevention device, advanced persistent threat notification mechanism, etc.
❖	All applications implemented as part of the Project shall undergo static and dynamic security testing before implementation and shall be continuously tested with respect to security on a regular basis at least once a year.
❖	All information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes like passwords).The authentication system used on these endpoint devices shall ensure that only authorized users are sending data over the network and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.

❖	Care shall be taken while transmitting confidential information over public networks to other government agencies with a prior permission from the concerned authority.
❖	Confidential information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes or CDs), shall be stored securely under lock and key.
❖	Unauthorized disclosure of data shall be protected when computers are sent out for repair or used by others within or outside ICCC and the data could be deleted. All data stored on hard disks shall be backed up and erased via user-transparent processes.
❖	All the internet activity shall be logged and monitored, and appropriate network devices shall be deployed so that access controls and related security mechanisms could be applied.
❖	Any system attacks should be well defended at device level and overall system level and shall include anti-virus mechanism. All system logs shall be properly stored and archived for future analysis.
❖	Data Security System shall be able to provide a complete network management for the Client. It shall monitor and report the performance, utilization, status, vulnerabilities and failures in the network in real time. It shall also monitor and manage access control and policy, security breaches and shall prevent detects and attacks on the network.
Data Integrity:	
❖	Data integrity must be ensured with a high level of requirement.
❖	Stability of data over time and in the procedures of physical media data shall be guaranteed and the protection of data content shall be ensured.
❖	Audit Trails: The application shall allow the management of compliance audit following the international standards for as appropriate for a Smart City.
❖	All acts of creation / modification / deletion must be registered with user identification and time stamp. Additionally, there must be an auditable trace of user sign-on and user sign-off with details of IP Address, Date, and Time etc. The records must be accessed using specific and legible statements irrespective of the programming language.

Functional Requirements Host Intrusion Prevention System (HIPS)	
❖	Solution should support stateful Inspection Firewall, Antimalware, Deep Packet

	Inspection with HIPS, Integrity Monitoring and Recommended scan in single module with agentless and agent capabilities and Firewall should have the capability to define different rules to different network interfaces with stateful inspection.
❖	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should Support CVE cross referencing when applicable for vulnerabilities.
❖	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers.
❖	The solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.
❖	Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window. Solution should have capability to submit unknown files to sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to server security solution and sandboxing should have at least virtual instance of server class OS - Win 2008, win 2012.
❖	HIPS should have signatures for known & unknown vulnerabilities and exploits. It should also allow for creation of custom signatures to secure home grown legacy applications. Detailed events data to provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit, should be logged.
❖	Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.
❖	Should provide automatic recommendations against existing vulnerabilities, Dynamically tuning IDS/IPS sensors (Eg. Selecting rules, configuring policies, updating policies, etc.) And provide automatic recommendation of removing assigned policies if vulnerability no longer exists - For Example - If a patch is deployed unwanted signatures should be un-assigned.
❖	The solution should have Application Control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules will be used to identify malicious software accessing the network and provide insight into suspicious activities.
❖	Solution should have Security Profiles allows rules to be configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers
❖	Solution should have Security Profiles allows Integrity Monitoring rules to be

	configured for groups of systems, or individual systems. For example, all Windows 2012 servers use the same operating system rules which are configured in a single Security Profile which is used by several servers. However, each server has unique requirements which are addressed at the individual Host configuration level.
❖	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and Solution Should have pre and post execution machine Learning and should have Ransom ware Protection in Behaviour Monitoring.
❖	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.
❖	Solution should have feature to take backup of ransom ware infected files and restoring the same and Management Server should support Active Passive high availability configuration. Should have central management console for server security and Anti-APT with sandboxing for central visibility and control.
❖	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless.
❖	HIPS Solution Should not have the need to provision HIPS Rules from the Policy Server as the Rules should be automatically Provisioned.
❖	Virtual Appliance should be able to build scan cache of VM which is scanned to compare the same file attributes while scanning other VM's thereby reducing the scan time and Should have the ability to identify resource usage of VM's during scheduled scans to avoid scan storms.
Endpoint protection and storage protection	
❖	Endpoint solution should have capability of AV, Vulnerability protection, HIPS, Firewall, Device control, virtual Patching and integrated DLP and pre and post machine learning execution.
❖	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability.
❖	Endpoint solution should have pre and post execution machine learning and behaviour monitoring along with ransom ware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same.
❖	Endpoint solution should have integrated DLP with pre-defined templates for HIPAA, PCI-DSS, and GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based for data loss presentation.
❖	Solution should have capability to submit unknown files to sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to Endpoint security solution to block and clean threats and

	sandboxing solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing with at least 60 virtual instances running in single sandboxing box.
❖	Endpoint solution should be in Gartner leader's quadrant from last 5 consecutive years.
❖	Host IPS should be capable of recommending rules based on vulnerabilities on endpoint and Host IPS should have dynamic rules based on System posture and endpoint posture
❖	Solution should deprovision corresponding HIPS rules id System upgraded or patched and Should support Detecting and Blocking Reconnaissance on the endpoint
❖	Solution should be APT ready, capable of submitting to Sandbox for analysis without additional License on Endpoint
❖	Server protection for storage solution should provide alerts to administrators for virus outbreaks and emergencies to help reduce response time
❖	Server protection for storage solution should support atleast ICAP, EMCCAVA, and RPC protocols.
❖	Server protection for storage solution should atleast supports EMC Celerra, Isilon, and VNX/VNXe storage servers, NetApp ONTAP filers and IBMN Series running Data ONTAP and Data Systems NAS
❖	Server protect for storage solution should provide automatic, incremental security updates and centralized management of servers via a web based console.
❖	Server protection for storage solution should provide real-time server protection against viruses, worms, spyware, and Trojan attacks.
❖	Server protects for storage should Integrates tightly with NetApp Filers or Hitachi NAS Platform and enables multiple or single scan server malware protection.
Network based Intrusion Prevention System (NIPS)	
❖	Intrusion Prevention System (NIPS) should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution.
❖	The proposed IPS underlying OS must be based on the proprietary OS and not general purpose OS such as Windows, Linux or Unix OS.
❖	The proposed IPS should be capable of trusting traffic and bypassing it by configuring rules in hardware layer
❖	The proposed IPS should support "IPS on a stick" in the Core switch by using VLAN Translation that allows customers to inspect inter-vlan traffic without adding additional in-line IPS per VLAN.
❖	Must support full redundancy solution (Active-Passive, Active Active)
❖	The proposed IPS must able to operate in Asymmetric traffic environment with DV filters protection
❖	High Availability must be supported without any synchronization and proposed

	IPS must support Dual Power Supplies
❖	IPS must have a power failure bypass modular that can support hot swappable function which allows traffic to bypass even after a modular get unplugged out of IPS Box during the RMA procedures
❖	The proposed IPS solution must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors
❖	The proposed IPS solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters
❖	The proposed IPS must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime
❖	The proposed IPS must have real 10Gbps throughput with atleast 60 million concurrent sessions and 450,000 new connections per second with <40 ms latency.
❖	The IPS vendor should be IPv6 certified by Join Interoperability Test Command (JITC)
❖	The IPS vendor must be position as a leader in vulnerability research by the latest Frost and Sullivan vulnerability tracker
❖	The IPS vendor should be in Gartner leader's quadrant in latest report. IPS vendor must be in the recommended products in the latest NSS report.
❖	The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace(Packet Capture), Rate Limit and Quarantine
❖	The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic
❖	The IPS filters must be categories into the following categories for easy management :- Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities, Network Equipment, Traffic Normalization, Peer to Peer, Internet Messaging, Streaming Media
❖	The proposed IPS must be able to support granular security policy enforcement based on the following methods: Per IPS device (all segments), Per physical segment unidirectional and bi-directional, Per 802.1Q VLAN Tag unidirectional and bi-directional, Per CIDR IP address range, Per 802.1Q VLAN Tag and CIDR as well, Firewall policy per security profile
❖	IPS solution must have vulnerability based filter which are known for most effectively for Zero Day Attack Protection and ZDI technology should be inbuilt.
❖	The proposed IPS should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods
❖	The proposed IPS must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc
❖	The proposed IPS must be able to support GTP inspection for GPRS/3G mobile networks
❖	The proposed IPS must be able to support 'VLAN Translation' feature which

	allows IPS to be deployed on a stick(out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment
❖	The proposed IPS must have the capability to convert other vendor's signature (such as snort).
❖	The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score
❖	The IPS vendor must provide 'the acknowledgement' data from the Microsoft security bulletin over the last 3 years to ensure that IPS vendor be the leader in the discovery of the zero day vulnerability in Microsoft product
❖	The proposed IPS solution must be able to provide zero day filters that must be included in weekly signature update
❖	The proposed IPS vendor must provide a global threat intelligence portal that provide real-time monitoring and statistics of malicious threats and attacks and NIPS should integrate with sandboxing to submit unknown files in sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to NIPS to block threats and sandboxing solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing with at least 60 virtual instances running in single sandboxing box.
❖	Must have the ability to view attack activities base on continent and countries and must have the ability to monitor and highlight recent new and growing threats with drill-down to view detailed threat source and destination data on each attack type
❖	NG IPS engine must be a smart enough to inspect the traffic based on condition (if then else). If the traffic is suspicious then it goes for the deep packet inspection
❖	NG IPS engine must be a smart enough to block the malicious traffic without further inspection on subsequent packets after the packets turn out to be a malicious traffic from the unknown traffic
❖	The proposed IPS must support an Out-Of-Band Ethernet management port and proposed IPS should support SSH2/Telnet and HTTPS/HTTP as a means of local management.
❖	The proposed IPS system must support SNMP and a private MIB that can be utilized from an Enterprise Management Application such as HP Open view, MRTG, etc.
❖	The proposed IPS system must be able to be managed locally independently without any centralised management server
❖	The proposed IPS system must support the option to send events in syslog messages, SNMP Traps and SMTP email messages within the need for a centralised management server
❖	The proposed IPS solution must support a centralized management server for enterprise management of the IPS devices.
❖	The centralized management server must be an appliance based on a harden

	OS shipped by default from factory and system shall allow the latest update to be manually, automatically or based on schedule
❖	The proposed management system shall allow the distribute of latest update manually, automatically or based on schedule to the various IPS devices
❖	The proposed management system shall also be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.
❖	The central management server should serve as a central point for IPS security policies management including versioning, rollback, import and export (backup) tasks.
❖	The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS Report
❖	The management server must support the archiving and backup of events and export to NFS, SMB, SCP and SFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.
❖	The proposed management system shall be able to provide different level of users account and access management. It shall provide at least 3 level - Super User, Administrator and User and The proposed management system must support Active Directory for user ID correlation
❖	The proposed management system must be able to support the syslog CEF format for SIEM integration and must support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis
❖	The proposed management system must support 3rd party VA scanners(Qualys,Foundstone, Nessus) to fine tune the IPS policy
❖	The proposed management system shall have a big data engine that allows customers to provide faster security analytics and faster report generation
❖	The proposed management system shall support the drill-down events from the report templates, such as drill-down from top 10 attacks over the one year report
❖	The proposed management system shall support 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered
❖	IPS solution should have machine Learning to detect exploit kit landing page and bypassing traffic for IPS internal issues(memory hang, firmware crash etc)
Anti-APT	
❖	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.
❖	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files

	and/or other objects.
❖	Solution must be custom built Anti-APT solution and must not have network perimeter security component part devices like firewall and IDS/IPS
❖	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network
❖	Upon detection of the threat, the proposed solution should be able to perform behaviour analysis for advance threats.
❖	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.
❖	Solution should provide risk based alerts or logs to help prioritize remediation effort.
❖	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.
❖	The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox.
❖	The proposed solution should use customizable OS sandboxes for detecting zero day malwares, This should not be a CPU or chip based function.
❖	Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.
❖	The proposed solution should be able to support XFF (Forwarded- For) to identify the IP Address of a host in a proxy/NAT environment.
❖	Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.
❖	Solution deployment should cause limited interruption to the current network environment.
❖	The proposed solution should able to work with the existing technologies for advance threat protection through web protocol.
❖	The proposed solution should be able to detect lateral movement (East West) of the attacker without the need of installing agents on endpoint/server machines.
❖	The proposed solution should support at least 100+ protocols for inspection.
❖	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
❖	The Proposed solution should be able to support up to 5 network segments on a single appliance.
❖	The proposed solution should be able to identify and help understand the severity and stage of each attack.
❖	The proposed solution should have built in capabilities to add exceptions for detections.
❖	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.
❖	The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal

	direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device
❖	The proposed solution should have an built in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.
❖	The Proposed solution should have a Correlation engine to automatically correlate across multiple protocol, multiple sessions and volume traffic analysis.
❖	The Proposed solution must provide a web service interface/API for customer to customize integration.
❖	The Proposed solution must have capabilities to correlate the detections on the device itself.
❖	The Proposed solution should support remote packet capturing for Kerberos traffic from the remote location for analysis.
❖	The Proposed solution should monitor Inter-VM traffic on a Port Mirror Session.
❖	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.
❖	The proposed solution should integrate with web security solution to block threats coming via HTTP, HTTPs and FTP
❖	The proposed solution should have an endpoint security component and should have following functionalities (Antivirus, antimalware, ransom ware protection, Vulnerability Protection in endpoint, integrated DLP and C&C detection, ability to quarantine and clean the infected files, ability to integrate with Anti APT components and automatically block/Quarantine zero day malwares by sharing Indicators of Compromise.
❖	The proposed solution should be able to run at least 60 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis
❖	Endpoints should be able to submit suspicious files directly to the on premise customized sandbox solution without the need to be intercepted by network based security solutions.
❖	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008 & 2012) and must have the capability to analyse large files and must be able to support more than 40MB file size.
❖	The solution should allow administrator to categorize files as safe based on Hash values (MD5) and proposed solution should be able to provide customizable sandbox to match customer's endpoint environments.
❖	Solution should have multiple built in virtual execution environments within single appliance to simulate the file activities and find malicious behaviours for advanced threat detection.
❖	The Proposed solution should support customizable Windows 7/8/10 and Microsoft 2008/12 operating environments for Sandboxing. This requirement

	should be based on virtual execution and should not be Hardware or chip based function.
❖	The proposed solution should have capability to scale out the detection when the bandwidth increases in future.
❖	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp
❖	The proposed solutions have the capability to perform tracking and analysis of virus downloads and suspicious files and proposed solution should support atleast 5 Ethernet Interfaces.
❖	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing and solution should have capabilities to scan inside password protected Archive and should have capabilities to detect Malwares and Spywares on windows and non-windows platforms.
❖	The proposed solution should have option to configure unrestricted internet for sandboxes and proposed solution must have capabilities to detect Mac, Linux and mobile malwares.
❖	The Proposed solution should have capability to detect attacker behaviour within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..)
❖	The Proposed solution should be able to Identify suspicious embedded object in document file like OLE & Macro extraction, Shellcode & exploit matching.
❖	The Proposed solution should have option to share Indicators of compromise for mitigation and clean up with AV endpoint and Web gateway to block threat at web gateway level and network level through NIPS. Anti-APT solution should share intelligence with endpoint, security web gateway solution, HIPS- server security & NIPS, similarly endpoint and security web gateway, NIPS & HIPS(Server Security) should submit files to AntiAPT solution for analysis and all three (Anti-APT, Web Security, Email security, Endpoint, HIPS (server security) solution should manage through single management console.
❖	The proposed solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link graph, geo-map, chart, tree map/pivot table.
❖	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
❖	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.
❖	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.

Firewall

❖	Firewall shall consist of stateful firewall and stateless filters.
❖	Firewall shall have the capability for proactive network attack detection.
❖	Firewall shall prevent replay attack.
❖	Firewall shall have min. 6 10/100/1000 Base-T GE ports; 4 x 10G SFP+ ports and shall be expandable as required.
❖	Firewall shall have a unified access control with functionalities such as: • TCP reassembly for fragmented packet protection • Brute force attack mitigation • SyN cookie protection • Zone based IP spoofing • Malformed packet protection
❖	Firewall shall have an Intrusion Prevention System (IPS) with following features: • Stateful Operation: ➢ TCP Reassembly ➢ IP Defragmentation ➢ Bi-directional Inspection ➢ Forensic Data Collection ➢ Access Lists • Signature Detection: ➢ Customer signatures creation ➢ Custom signatures ➢ Dynamic signature update ➢ Automatic signature sync • Alerts and updates: ➢ Alerting SNMP ➢ Log File ➢ Syslog ➢ E-mail ➢ Daily and emergency updates • Security Maintenance: ➢ 24/7 Security Update Service ➢ Real-time and History reports of Bandwidth usage per policy

	➢ Protocol anomaly detection ➢ IPS attack pattern obfuscation ➢ User role based policies ➢ User based application policy enforcement ➢ Provision for external bypass switch
❖	Firewall shall have following user authentication capabilities: • Third party user authentication: RSA secure ID, LDAP, RADIUS • RADIUS accounting • XAUTH VPN, Web based, 802.X authentication • PKI certificates
❖	Firewall shall have the following minimum capabilities: • VPN functionalities with 2000 simultaneous VPN tunnels • Encrypted throughput: minimum 800 Mbps • Concurrent connections: up to 100,000
Antivirus	
❖	Antivirus shall be able to detect and block malicious software in real time, including viruses, worms, spyware, Trojan horses, adware, and Rootkit etc. It shall provide zero-day detection technology.
❖	Antivirus shall protect the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and stability.
❖	Antivirus shall be able to identify infections by name, category, severity, hosts and user etc.
❖	Antivirus shall be able to report Bot incidents by specific malicious activity (spyware, IP scanning, spam etc.). The antivirus shall have built in intelligence and co-relation capability to inspect, detect and block active and dormant bots.
❖	Antivirus shall be able to block devices based on Windows Class ID. Devices shall include USB, Infrared, Bluetooth, Serial Port, Parallel Port, Fire Wire etc. Antivirus shall block or give permissions for such devices.
❖	Antivirus shall protect transmission of data being sent to hacker system who has spoofed their IP or MAC address.
❖	Antivirus shall scan email traffic including email client like Outlook.
❖	Antivirus shall include content filtering and data loss prevention.

❖	Antivirus shall have features to prevent peer to peer sharing, streaming media, games and other applications from internet.
❖	Antivirus shall have built in URL filtering.
❖	Antivirus shall provide standard and customized reports.

SIEM (Security Incident & Event Management)	
❖	Solution should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.
❖	The solution should factor with following minimum components: • Management & Reporting • Normalization and Indexing • Correlation Engine • Data Management
❖	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department. The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required
❖	The solution should provide an integrated dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.
❖	Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc.
❖	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement; normalization should be performed to meet the reporting and analysis needs.
❖	A single log appliance should support minimum 30,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces. Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 100,000 EPS.
❖	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration. Should store RAW packet DATA for 7 days and

	normalized packet data for 30 days for forensics.
❖	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions. Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.
❖	The proposed solution must be able to provide the complete platform to perform Network forensics solution
❖	The solution must be able to detect malicious payload in network traffic • Detect and reconstruct files back to its original type • Detect hidden or embedded files • Detect and flag out renamed files

6 OEM Professional Services for Project Implementation

Both the bidder and the OEM shall have to deploy professional services resources to implement and manage the project. The following requirements are required to be met. All resources from OEM and Bidder are required to be their own resources; i.e. all resources required from the OEM should be directly from the OEM and the same for the bidder. As a part of the build phase, it is in the best interest of project for OEM to be accountable for the configuration and deployment, which should happen as per the high level design done by the Master System Integrator. Therefore, the SI should use the OEM to deliver the network wide low level design, the device level configurations and acceptance plan. This will ensure that the product & technology supplied by respective OEM work the way it is committed by the MSI.

MSI & OEM's Professional Services Offerings should bring the following to Customer:

(1) Provides a full range of implementation services, including project management, project engineering, and configuration, staging, and rollout coordination, to ensure that Solution deployments are seamless and scalable.

(2) The Scope of Work has been described in the Sections below.

(3) The MSI shall build a high-performance network that will operate at best efficiency all the time. Only seamlessly integrated network architecture with focused

engineering support can consistently deliver quality of service, reliability, availability, and security.

(4) MSI should provide the overall program management to ensure that the complete solution, which may include multiple technologies from respective OEM, work together seamlessly as per the design goals. The MSI should further ensure that a robust support model is put together in such a way that the Solution runs with the level of availability it is designed for and with a predictable restoration time in case of any failures.

(5) The OEM should complement the MSI by providing the OEM specific Planning, designing (Low Level Design, Implementation planning, Device Level Configuration etc.) expertise to make sure that there supplied technology & products work as per the design objectives.

(6) MSI along with the OEM shall be responsible for rolling out project under the scope of this document with shortlisted bidders & their partners.

Technology planning & Design

The life cycle of the PROJECT will begin with the various planning stages associated with Architect deployment. The OEM must consider many factors such as available bandwidth, resiliency and recovery, quality of service (QoS) and rollout planning and then build an appropriate technology plan. OEM shall be responsible to plan; design and program manage the complete Implementation for initial period (6 months). After completion of the technology plan, the technical design of the Solution elements will be defined. OEMs Professional Services engineering team shall consult Customer/ MSI Solutions team to help them meet these goals by preparing the design documentation.

Implementation

Once the design is completed and the required activities have been identified; the physical rollout of product should commence. MSI will use trained and highly skilled ecosystem engineering team or integrators to carry out the implementation. And OEM to be responsible for below:

The OEM shall be responsible for the following:

Project Management for complete implementation phase

(1) Low Level Design Development
(2) Solution Implementation Plan Development
(3) System Acceptance Test Plan Development
(4) Implementation of Core Setup

The MSI shall be responsible for the following:

(1) Complete Implementation services
(2) Operation & Maintenance Services

OEM Services Completion

A final letter to be submitted by the MSI confirming that the complete design has been prepared by the OEM in consultation with the MSI and the same has been correctly implemented by the MSI. This letter should be jointly signed by the MSI as well as the OEM. This is to ensure that OEM Delivery resources participation during Project Phase.

7 Handholding and Training

In order to strengthen the staff, structured capacity building programs shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for Command Control Centre/City Operation Staff and designated Authorities & Police staff shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of such operation centres. These officers shall be handling emergency Situations with very minimal turnaround time.

- MSI shall prepare and submit detailed Training Plan and Training Manuals to Authority/authorized entity for review and approval.
- Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees,

course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.

- MSI shall be responsible for necessary demonstration environment setup of all ICT solutions in this RFP to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at Operation centres data centres & field Locations. End user training shall be conducted at a centralized location or any other location as identified by Authority with inputs from the MSI.
- MSI shall conduct end user training and ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system.
- MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
- MSI shall prepare the solution specific training manuals and submit the same to Authority for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English & Hindi language.
- MSI shall provide training to selected officers of the Authority covering functional, technical aspects, usage and implementation of the products and solutions.
- MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
- An annual training calendar shall be clearly chalked out and shared with the Authority along with complete details of content of training, target audience for each year etc.
- MSI shall update training manuals, procedures manual, and deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.

- The MSI shall ensure that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by the MSI.
- Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the MSI.
- Time Schedule and detailed program shall be prepared in consultation with LSCL and respective authorized entity. In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
- MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- Authority shall be responsible for identifying and nominating users for the training. However, MSI shall be responsible for facilitating and coordinating this entire process.
- MSI shall be responsible for making the feedback available for the Authority/authorized entity to review and track the progress, In case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the MSI shall re-conduct the same training at no extra cost.

Types of Trainings: Following training needs is identified for all the project stakeholders:

1. **Basic IT training**

   This module shall include components on fundamentals of:

   - Computer usage,
   - Network,
   - Desktop operations,

- User admin,
- Application installation,
- Basic computer troubleshooting etc.

2. Initial Training as part of Project Implementation

I. Functional Training:

- Basic IT skills
- Software Applications
- Networking, Hardware Installation
- Centralized Helpdesk
- Feed monitoring

II. Administrative Training:

- System Administration Helpdesk, FMS, BMS Administration etc.
- Master trainer assistance and handling helpdesk requests etc.

III. Senior Management Training:

- Usage of all the proposed systems for monitoring, tracking and reporting,
- MIS reports, accessing various exception reports

3. Post-Implementation Training

- Refresher Trainings for the Senior Management
- Functional/Operational training and IT basics for new operators
- Refresher courses on System Administration
- Change Management programs

8 Project Implementation Timelines & Deliverables:

LSCL intends to implement the project in phased manner approach, distributed in three phases as mentioned below:

Mobilization and Kick start: T + 1 month (*T is the date of Signing of the contract with MSI)*

i. Study & Reporting Activities (T is the date of Signing of the contract with MSI)

Phase 1	Activity	Time in months
Resource	➢ Resource Mobilization	T+0.10 months

Mobilization	➢ Inception Report	
Detailed Project Study for all ICT solution proposed	➢ Detailed Survey of Sites Identified ➢ Hardware Deployment plans ·If Any ➢ Detailed Project Plan including Operations management, Contract management, Risk management, Information Security and Business Continuity etc. ➢ FRS , SRS , SDD etc Documents for all work streams	T+1 months

ii. Phase 1 System Implementation – T+3 Months (T is the date of Signing of the contract with MSI)

No	Smart Solutions	Milestone period	Activity
1.	Unified Smart Mobility Card	1-3 month	• Integration of LMRC card with Municipal • Development of all concerned Applications and installation of field devices in 100% of the identified junctions and shall be on Go Live
2.	Environmental Sensors & Variable Message Sign	1-3 month	
3.	Setting up of DC & DR	1-3 month	
4.	LSCL Website	1-3 month	Migration and hosting of the website on LSCL Server alongwith Strengthing & augmentation of existing website.

iii. Phase 2 T + 6 months (T is the date of Signing of the contract with MSI)

No	Smart Solutions	Milestone period	Activity
1	Command and control Centre	1-6 Month	• Sizing of CCC and preparation of use cases • Application go live
2	LSCL Mobile App		
3	Geographical		

	Information Systems (GIS)/ GIS City Portal		• Development and deployment of all concerned equipment's and Applications
4.	Drishti City Surveillance		
5.	UP Dial 100		
6.	Biometric Attendance System		
7.	ICT based Solid Waste Management System		
8.	GPS Tracking of Vehciles		
9.	e-Governance		
10.	Other Solutions as a part of this RFP (Future integration will be taken as and when such projects will be implemented)		

iv. Phase 3 – T1 + 60 months (T1 is the date of Go Live of all application)

Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution.

Operation & Maintenance	SLA Compliance Report	Every Quarter

9 MSI Scope of Work:

The Master System Integrator (MSI) shall broadly cover the following main scope of services:

- Survey
- Design
- Supply

- Install
- Test
- Integrate,
- Commission
- Training & Capacity Building
- Operations and maintenance

MSI shall be responsible to carry out any detailed survey prior to submission of bid for the complete solution components required to finalize infrastructure requirement, network bandwidth requirement, implementation, operational & administrative challenges etc.

MSI shall suggest the sizing of the required hardware necessary for meeting the required performance related SLAs starting from ”Complete Deployment” till the first Five years of productive use of the system. The MSI is responsible for sizing the proposed hardware for all the modules of LSCL in future and performance requirements of the solution. The MSI is to supply and install the hardware and systems software as part of the scope of work. The bidder shall ensure that the LAN / WAN, servers and storage are sized adequately with built in redundancy into the architecture to meet a 10 second response time in terms of performance. The MSI has to size and propose hardware requirements for the DR site including back up software as well. The subsequent sections detail out the scope with respect to each of the solution component. The MSI shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive. MSI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfill the requirements as mentioned in this RFP and factor the same in its response.

The following process presents the detailed scope of services that have to be carried out as a part of the contract.

9.1 Project Management

MSI shall be responsible for end to end project management for the implementation and maintenance of the smart city ICT components. MSI shall deploy a competent team of experts for project management which shall include a Project Manager. The Project Manager shall be the single point of contact that shall assume overall responsibility of the Project and ensure end to end working of the Project. He shall function as the primary channel of communication for all Client requirements to the implementation team. In case of any absence of the project manager

(sickness or vacation), the MSI shall ensure that an alternate project manager (as approved by the client or its representative) shall be provided during the absence period.

MSI shall be responsible for preparing a master schedule of work which shall highlight implementation plan for all the Project milestones. The schedule shall identify the manufacture, delivery, installation, integration of equipment (Software and Hardware), training programs, test procedures, delivery of documentation and the respective solutions. The schedule shall also show Client and any third party responsibilities along with the activities in the timeline. MSI shall conduct bi-weekly meetings between the Client (and its representative) to discuss project progress and implementation in Lucknow. All key personnel associated with the project shall also be available for meetings whenever asked by the Client or its representative. MSI shall also be responsible for effective risk and issue management and escalation procedures along with matrix as part of project management. MSI shall identify, analyse, and evaluate the project risks and shall develop cost effective strategies and action plan for mitigation of risks. As part of the Project MSI shall monitor report and update risk management plans and shall be discussed during project meetings. All the tools required by MSI for project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI. All deliverables shall be submitted in at least two (2) formats i.e. draft and final. The practice of submissions for all deliverables will be that three (3) hard copies and CDs of every deliverable shall be submitted. The submissions will include both hard and soft copies.

9.2 Prototype Acceptance and Factory Acceptance Testing

After the approvals of the technical data sheets by the Client or its representative, MSI shall submit the prototype of all the material presented in the Detailed Design Report to the Client for its review and approval. Note that it shall be MSI's responsibility to get the prototypes approved in due course of time without affecting the overall schedule of completion of works. Material provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT). Details regarding the PAT and FAT are presented in Testing Section of the Scope of Work. MSI shall also present to the Client and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The client at its own discretion shall visit any FAT site.

9.3 Hardware Supply and Installation Stage

MSI shall be responsible for the supply and installation of all components as part of the Lucknow smart city solutions to meet the technical, functional, business and performance requirements of this RFP. No deviations from these requirements shall be acceptable by the client. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and provided by the MSI. MSI shall deliver the project and install and handle the equipment in accordance with manufacturer's requirements. Installation process of the MSI shall be flexible and shall accommodate Client's requirements without affecting the schedule as specified in the RFP.

MSI shall be responsible for all supply, storage and handling of the material provided as part of the bid document. The OEM proposed for the IT infrastructure shall be in line with the national security policy (as applicable).

If there is removal/change of any existing material during installation process and belongs to the Client, the material shall be handed-over to the Client. MSI shall also be responsible for reinstating any site in the project limits at no additional cost to the client. It shall be the MSI's responsibility to supply and install all hardware in compliance with the requirements of the RFP. MSI shall be responsible for all implementation works on the project including any civil, structural, electrical, etc. works required to meet the requirements of the project. All power conversions necessary to operate the equipment shall be under the scope of MSI.

9.4 Software Development

MSI shall be responsible for development and deployment of all software required to meet the requirements of the project. It is preferred that majority of the software shall is time tested and pre-configured. However, some of the modules may require bespoke development. MSI shall be fully responsible for developing and implementing all software required for the project. This software shall be developed based on the approved software and functional requirements specifications. The technology platform chosen for all software shall be based on industry

standards based and shall be secure. Migration of data shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration. All licenses for the software shall be perpetual and the client may purchase any additional licenses at the stated cost (as per financial proposal of the Bidder) during this course of the contract. The MSI shall ensure that full support from the OEM's is provided during the course of the contract. MSI shall be responsible to provide any upgrades, patches, fixes to the software during the course of the contract at no additional cost to the client.

9.5 System Integration

MSI shall be responsible for the integration of all hardware and software supplied as part of this Project as per the technical and performance requirements of this bid document. The system integration scope also includes integration of the Project components with the components provided by others as per the details of the RFP. In case the integration of any of the systems is not as per the requirements specified in the bid document, MSI shall be responsible to provide any upgrades required to meet the Integration requirements at no additional cost to the Client unless otherwise agreed by the Client. It shall be the responsibility of MSI to take approval of the Client for the Integration of the overall system as per the bid document. Post systems integration, the Client shall review and approve the overall performance of the integrated system as per the requirements of the bid document. MSI shall be responsible for fixing any requirements that are not found in compliance with the original bid requirements and approved detailed design at no additional cost to the client.

9.6 Testing

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in this document and will be subject to Client or its representative's approval. The testing shall include any existing civil infrastructure equipment or materials to be taken over by the MSI. Approvals or passing of any inspection by the Client shall not, however, prejudice the right of the Client or its representative to reject the material if it does not comply with the specification or requirements of the RFP when erected or give complete satisfaction in service. The MSI shall design and successfully complete tests to demonstrate that all

equipment, materials and systems furnished and installed function in the manner intended and in full compliance with the requirements outlined in the RFP and the approved detailed design of the MSI. All tests shall be subject to inspection or witnessing of tests by the Client or its representative. Inspection or witnessing of tests may be waived at the sole discretion of the Client or their representative, subject to the MSI furnishing the Client or their representative with properly completed test certificates in accordance with the requirements of the RFP. Failure of the Client or their representative to witness any test shall not relieve the MSI of the obligation to meet the requirements of the Contract. MSI shall submit an Acceptance Test Procedures document (ATP), for Client's approval prior to undertaking any testing. The ATP shall clearly address:

- ✓ Type of testing and device to be tested;
- ✓ How each testable specification requirement will be demonstrated, including the test environment and set-up, specific functionality to be tested, method for performing the test and quality assurance procedures;
- ✓ The results that will constitute success for each test;
- ✓ Timing of test within the overall Contract schedule;
- ✓ The location for testing;
- ✓ Personnel required to conduct the test;
- ✓ Approximate time required to execute the test or set of tests;
- ✓ Responsibilities of both the MSI and Client's representatives during each test; and
- ✓ A cross-reference to which Contract requirements from the Compliance Matrix (to be developed by the MSI) are being addressed by each test procedure.

The ATP shall include an updated Compliance Matrix to include the test relevant stage at which each contract requirement will be demonstrated; and a cross-reference to the test procedure(s) that serve to address each contract requirement. The Compliance Matrix shall be used as a "punch list" to track which requirements have not yet been

demonstrated at each stage of testing. A requirement classified as having been "demonstrated" during a certain ATP stage can be subsequently redefined as having been "not demonstrated" if compliance issues emerge prior to System Acceptance. ATP shall be submitted to Client at least two (2) weeks in advance of any intended testing. All measuring instruments required to measure test parameters shall be calibrated by an approved testing authority. The equipment shall be inspected for standards of construction and electrical and mechanical safety. Test results shall be recorded for all tests conducted under this Contract. The MSI shall make test results available to Client or their designate for review immediately after completion of the tests. ATP for each test shall be collated, bound and delivered as part of the close-out documentation requirements specified herein. ATP submission shall include a hard copy of the originally marked test results and a neatly typed summary. Two (2) hard copies and one (1) electronic copy shall be provided.

ATP shall incorporate the following distinct stages for each deployed stage:

- **Prototype Acceptance Tests (PAT)**: Prototype Approval Test shall be conducted only on the customized equipment for their design and compliance to functional specifications. PAT shall be completed before conducting FAT and only after approval of PAT by Client's representative, the equipment shall go in production. PAT shall be witnessed by Client's representatives;
- **Factory Acceptance Tests (FAT)**: FAT shall be conducted before the equipment and software is shipped to Client for installation, and deficiencies shall be rectified before shipping to Client for installation. All devices furnished by the MSI shall be tested and subjected to a nominal 72-hours burin-in period at the factory. FAT shall be witnessed by Client's representatives at their discretion. Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected;

- **Pre-Installation Testing (PIT):** All equipment supplied under this Contract shall undergo pre-installation testing in accordance with the ATP. This shall include existing equipment, any spare parts, any new equipment provided by Client or their designate and new equipment provided by the MSI.

If the equipment is considered a standard production item, the MSI may, with the prior consent of the Client or their designate, supply a copy of the equipment manufacturer's quality control test results in place of a MSI performed test.

All PIT testing shall be carried out prior to installation of the equipment. After satisfactory completion of the MSI's PIT tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.

- **Installation Acceptance Tests (IAT)**: IAT shall be conducted after each installation of each equipment type, and deficiencies shall be rectified before the initiation of IAT. IAT may be witnessed by Client's representatives;
- **Proof of Performance Testing (POP):** The MSI shall implement a structured proof of performance testing, which will progressively place all components in service. Site tests shall be performed on individual components, subsystem sites, and the complete subsystems, as necessary to confirm that each element of the system functions satisfactorily and fulfils the requirements of this specification.

Completion, submission, and approval of all relevant PIT and IAT tests and results must be completed prior to carrying out any POP tests.

All subsystem equipment and components shall be tested by the MSI regardless of whether or not it is a standard item.

After satisfactory completion of the MSI's POP tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.

- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified

in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the Client or their designate. This work will be carried out under the direction of the Client or their designate.

Completion, submission and approval of all relevant PAT, FAT, PIT IAT and POP tests and results must be complete prior to carrying out any SIT tests.

The MSI shall:

- ✓ Complete all equipment and subsystem tests required in the Contract;
- ✓ Test each subsystem independently on the communications subsystem;
- ✓ Add subsystems one at a time and monitor the overall performance;
- ✓ Fail safe testing of all subsystems one at the time while monitoring overall systems performance.

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system, together with final copies of all Operating and Maintenance Documentation for the System.

- **Stress and Load Testing:** Comprehensive stress and load testing of Smart Governance and Smart Connect modules shall be conducted to demonstrate robustness and reliability of the system.
- **Security Testing (including penetration and vulnerability test):** Security test shall be conducted to demonstrate security requirements at network layer and software applications. Components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for portal, mobile app, and other systems. Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory

requirement.

- **Pilot Test:** Requirements for Pilot Test is explained in the Pilot Deployment Section of the Scope of Work.
- **System Acceptance Tests (SAT)**: SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of Burn-in Test. SAT shall be conducted on full system completion only to determine if the system functional and technical requirements as specified in the bidding documents are meet. SAT shall be witnessed by Client's representatives. Data migration, if any will be carried out by MST prior to commencement of this stage. SAT shall also include any performance and load testing for the software applications.
- **Burn-in Tests (BT)**: Following successful completion of the SIT and SAT, the approved System will be put into service and its performance monitored for a period of Fifteen (15) consecutive calendar days for the purpose of verifying system reliability in an operating environment. Any failures and defects occurring in this time will be documented. Any serious defects which affect the availability of the system will be a basis for restarting the test. Upon the satisfactory completion of this performance testing a Completion Certificate will be issued.

The MSI shall not commence BT until SIT and SAT have been performed and successfully completed and all documentation of the successful completion of PAT, FAT, PIT, IAT, POP, SIT and SIT, along with notification of the schedule date of the BT is provided to the Client or their designate in accordance with the Requirements. Commencement of BT will be conditional on the Client or their designate providing written notification of Client's readiness to proceed to BT.

The MSI shall be suitably prepared for the BT prior to the start date. Repeated failure of the BT may result in the MSI having to reimburse the Client or their designate for costs incurred. No compensation to the MSI will be made for repeat testing.

Where equipment supplied by the MSI fails during the burn-in period, the MSI shall restart the test at day zero (0) following appropriate corrective measures.

If a utility failure is proved to be the cause of testing failure, then the MSI shall restart the Ten (10) day burn-in test at the day the failure occurred. If a subsystem failure is proved to be the cause of testing failure, then the MSI shall start the test over at day 0 (zero).

Where tests or burn-in indicate that an existing subsystem or component, not provided by the MSI, is defective, the MSI shall immediately report the deficiency to the Client or their designate. The Client or their designate may assign corrective repairs, retesting and repeat of BT to the MSI, in accordance with change provisions of the Agreement.

The MSI shall provide the Client or their designate with a contact name and phone number(s) for a designated emergency contact person during BT. The emergency contact person shall be accessible twenty-four (24) hour a day, for each day of testing.

Issuance of the Completion Certificate is a basis for the start of the Warranty period for the Systems.

- **Operational Acceptance Test:** Shall be conducted after successful SAT and Burn-in tests. Continuous fault free running of the System shall be tested. Post the completion of Operational Acceptance Test, System shall be considered for Operational System Acceptance and Defect Liability Period (DLP) shall commence. Operational Acceptance Test shall include the following as a minimum:

- Completion of all activities and fulfilment of all business, functional and technical requirements listed in RFP;
- Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc.;

Client may authorize the MSI to proceed to the next testing stage with certain deficiencies not yet resolved. The MSI shall provide written notice to Client at least five days in advance of any testing, indicating the specific tests to be completed as well as the date, time and location. The MSI shall be required to reschedule testing if Client witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

9.7 Pilot Deployment

The MSI shall conduct Pilot deployment and testing for meeting Client's business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on Client's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.

The Pilot shall be demonstrated to the Client's representatives. If for any reason the pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

9.8 Third Party Acceptance Testing, Audit and Certification

The primary goal of Acceptance Testing, Audit & Certification is to ensure that the system meets requirements, standards, and specifications as set out in this RFP and as needed to achieve the desired outcomes. The basic approach for this will be ensuring that the following are associated with clear and quantifiable metrics for accountability:

- Functional requirements
- Test cases and Requirements Mapping
- Infrastructure Compliance Review
- Availability of Services in the defined locations
- Performance and Scalability
- Security / Digital Signatures
- Manageability and Interoperability
- SLA Reporting System
- Project Documentation
- Data Quality Review

As part of Acceptance testing, audit and certification, performed through a third party agency e.g. STQC/ CERT-IN Empaneled agency, LSCL shall review all aspects of project development and

implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here, it is important to mention that there may be two agencies selected one for audit & certification of security and control aspect of the system and the other for audit & certification of overall applications. LSCL will establish appropriate processes for notifying the MSI of any deviations from defined requirements at the earliest instance after noticing the same to enable the MSI to take corrective action. STQC will be engaged by the Master System Integrator. Following discusses the acceptance criteria to be adopted for system as mentioned above:

- **Functional Requirements: -** The system developed/customized by MSI shall be reviewed and verified by the agency against the Functional Requirements signed-off between LSCL/Concerned Department Authority and MSI. Any gaps, identified as severe or critical in nature, shall be addressed by MSI immediately prior to the deployment of the system in production. One of the key inputs for this testing shall be the traceability matrix to be developed by the MSI from system. Apart from Traceability Matrix, agency may develop its own testing plans for validation of compliance of system against the defined requirements. The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (external audit) as well as the select internal department users (i.e. User Acceptance Testing).

- **Infrastructure Compliance Review: -** Third party agency shall perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure supplied by the MSI against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by MSI. Compliance review shall not absolve MSI from ensuring that proposed infrastructure meets the SLA requirements.

- **Security Review:** - The software developed/customized for system shall be audited by

the agency from a security & controls perspective. Such audit shall also include the IT infrastructure and network deployed for system. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the system for the following activities:

- ✓ Audit of Network, Server and Application security mechanisms
- ✓ Assessment of authentication mechanism provided in the application /components/ modules
- ✓ Assessment of data encryption mechanisms implemented for the solution
- ✓ Assessment of data access privileges, retention periods and archival mechanisms
- ✓ Server and Application security features incorporated etc.

- **Performance: -** Performance is another key requirement for system and agency shall review the performance of the deployed solution against certain key parameters defined in SLA described in this RFP and/or agreement between LSCL and MSI. Such parameters include request-response time, work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.
  - ✓ The MSI must provide System and Database Performance System for all servers in the Data centre
  - ✓ The MSI must provision for End-User response time monitoring and transaction based deep-dive analysis for Web based applications.
  - ✓ The MSI must provision for Integrated Performance Management System for Monitoring Networks, Systems & Databases.
  - ✓ The MSI must provide a Traffic Analysis and Reporting System for deep-dive diagnostics.

- **Availability: -** The system should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including

network, server, security, DC/DR fail- over tests to verify the availability of the services in case of component/location failures. The agency shall also verify the availability of services to all the users in the defined locations.

9.9 Final Deployment and Documentation

Post the final deployment, MSI shall handover detailed documentation that describes the site conditions, system design, configuration, training, as-built conditions, operation and maintenance. All documentation shall be in English and Hindi (as agreed with the client), shall utilize metric measurements, and shall be submitted directly to Client in paper hardcopy and electronically in Word/AutoCAD/Excel/Project and Adobe Acrobat that should be editable or updated. All installation drawings shall be prepared in AutoCAD, GIS and Adobe Acrobat and provided on CD-ROM as well as hard copies. The drawings shall contain sufficient detail including but not limited to equipment dimensions, interfaces, cable details, equipment mounting and fire protection. Electrical and electronic drawings shall be supplied to show engineering changes made to any component or module any time during the contract period.

'As-built' Documents delivered by the MSI shall include:

- An inventory of all components supplied including model name, model number, serial number and installation location.
- An inventory of all spare parts supplied including brand, model number, and serial number and storage location.
- All reference and user manuals for system components, including those components supplied by third parties.
- Point of Contact for each OEM for maintenance
- Warranties and Maintenance schedules for the hardware procured
- All warranties documentation, including that for components supplied by third parties
- As-built in CAD and GIS.
- A diagram indicating the as-built inter-connections between components
- Software documentation which also includes the version number of all software, including that supplied by third parties
- Cable run lists and schedules
- All network and equipment details such as IP addresses, user names, and passwords

- Data communication protocols; and
- 'As-Built' drawings for all components installed as per the scope of work mentioned in this RFP document.

MSI shall submit to the LSCL copies of comprehensive operating and maintenance manuals, and log sheets for all systems and hardware supplied as part of this RFP. These shall be supported with the manufacturer's operating and maintenance manuals. The manuals shall be complete, accurate, up-to-date, and shall contain only that information that pertains to the system installed.

9.10 Operational System Acceptance

At the completion of operational acceptance test, the system shall be considered for operational system acceptance. At the close of the work and before issue of final certificate of completion by the Client, the MSI shall furnish a written guarantee indemnifying Client against defective materials and workmanship for a period of one (1) year after completion which is referred to as Defect Liability Period. The MSI shall hold himself fully responsible for reinstallation or replace free of cost to Client during the Defect Liability period. MSI shall provide approved temporary replacement equipment and material such that the system remains fully functional as designed and commissioned during repair or replacement activities at no cost to the Client.

9.11 Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, up-gradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements of the Lucknow smart city solutions deployed as part of this project and shall maintain service levels as defined in the RFP. All equipment and material supplied by the MSI shall be provided with standard warranty against defects of design and manufacturing and against faults and failures associated with workmanship of MSI and its sub-contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the Client. MSI shall provide all the technical,

managerial, and other staffing required managing day- to-day maintenance of the Lucknow smart city solutions during the Contract period

All spares required for the smooth operation of the Lucknow smart city solutions shall be maintained by the MSI for the entire duration of the contract to meet SLA requirements. The cost of the spares, repairs, and replacement shall all be deemed to be included in the Price quoted by the MSI. MSI shall also institutionalize structures, processes and reports for management of SLA. Root cause analysis and long term problem solutions shall also be part of MSI scope. MSI shall maintain all data regarding entitlement for any upgrade, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates/upgrades and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the Client during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any changes/upgrades to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system.

10 Integration of Future IT initiatives

The solution should be scalable and modular in structure and should be able to integrate other future IT initiative of Lucknow Smart City which is not part of this RFP. The bidder should estimate and provide estimated cost of extra services integration in terms of man month rate (Rate Card). The Rate card will be valid for 5 (five) years. This rate card will be for extra work only and it should not be the part of commercial bid.

11 Payment Terms and Schedule

1. The request for payment shall be made to the Authority in writing, accompanied by invoices describing, as appropriate, the services performed, and by the required documents submitted

pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.

2. Due payments shall be made promptly by the Authority, generally within Sixty (60) days after submission of an invoice or request for payment by MSI
3. The currency or currencies in which payments shall be made to the MSI under this Contract shall be Indian Rupees (INR) only.
4. All remittance charges shall be borne by the MSI.
5. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
6. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
7. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

Payment Schedule

Payments to MSI, after successful completion of the target milestones (including specified project deliverables), shall be made as under: -

S. No.	Scope of Work	Timelines	Payment
1	Upon approval of SRS,FRS & SDD document by the authority	T+1 Months	10% of contract value
1.	Phase I Operationalization & Go Live Acceptance by the authority	T + 3 Months	30% of contract value
2.	Phase II Operationalization & Go Live acceptance by the authority	T + 6 Months	30% of contract value
3.	Operations & Maintenance phase for a period of 60 months from the date of Go Live of the last solution	T1 + 60 Months	30% of Contract Value in equal quarterly instalments

Note:

T is the date of Signing of contract

T1 is the date of Go Live of the last phase.

12 Annexure 1: Industry Standards

12.1.1 Annex-A (Biometrics Standard)

Biometrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.
It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.
In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.
Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.
This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.
If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of botheyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet

4:2005(E)	specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

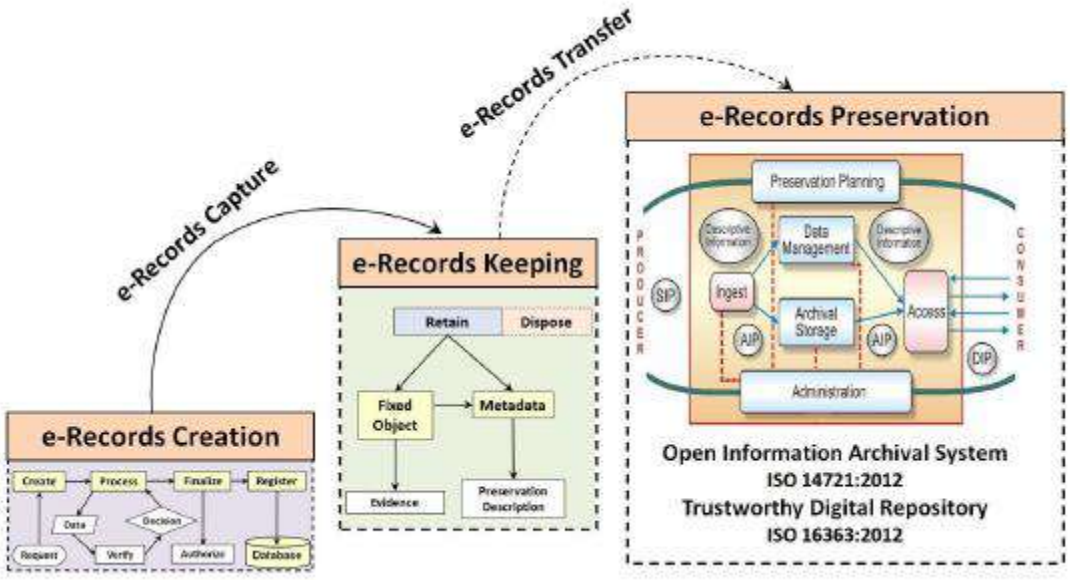
12.1.2 Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of Open Type fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard

	○ Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of Deity.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, Deity.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

12.1.3 Annex-C (Localisation and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard.The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode	Unicode Consortium, Inc.	Matured	Mandatory

	consortium from time to time.			

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.
Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646
Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.
Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible witheach other, is causing serious problems in information exchange

amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)
A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)
OFF fonts allow the handling of large glyph sets using Unicode encoding. Suchencoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, whichenable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

12.1.4 Annex-D (Metadata and Data Standards)

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

Rerefrence Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

12.1.5 Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. Creation of Mobile Services Delivery Gateway (MSDG)

MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. **Guidelines to deliver public services round-the-clock to the users using m-Governance**

b. **Guidelines to develop standard based mobile solutions**

c. **Guidelines to integrate the mobile applications with the common e-Governance infrastructure**

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILE SEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

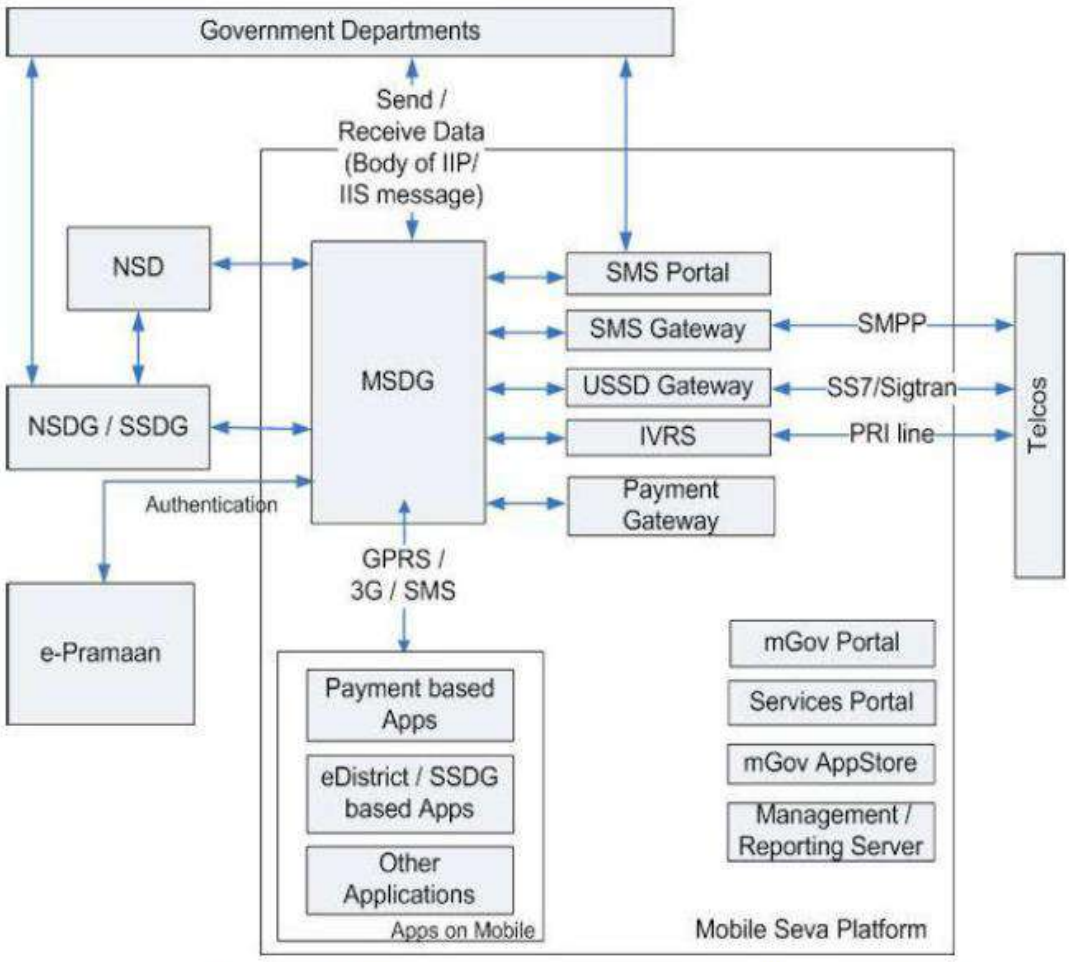


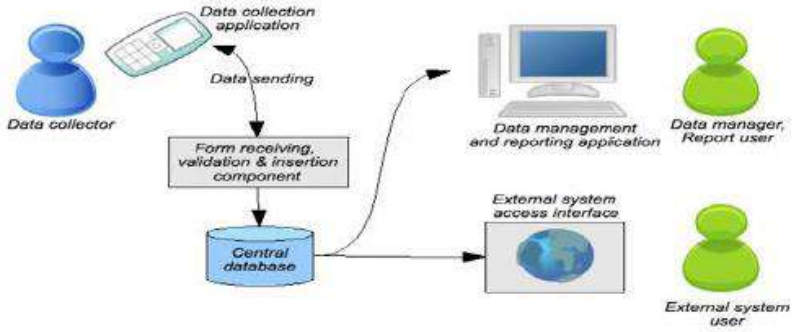
Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**
   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**
   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:



The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

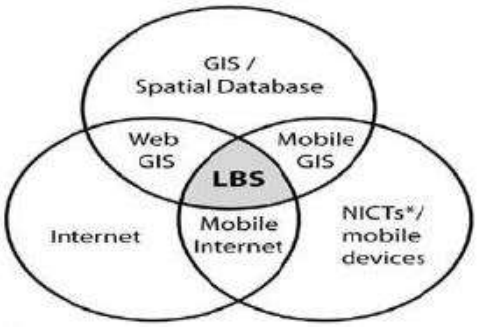
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.
Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.
It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.
A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**
b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Althoughefforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.
An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.
To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.
Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver's mobile number and MMID, and the amount of funds to transfer.
IMPS will authenticate the sender, check the receiver's mobile number and MMID, and transfer the funds to the receiver's account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.
Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone's screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.
With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

12.1.6 Annexure-F (GIGW)

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code

provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the searchengines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the searchengine results. Further, it is important since the screen readers used by the visually impaired

users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.
b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.
As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.
Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php
Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.
Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.
The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.
If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper

link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

12.1.7 Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the "Policy on Open Standards for e-Governance" and "Technical Standards on Interoperability Framework for e-Governance".

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India" (hereinafter referred to as the "Policy") will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government's approach on the use of "Open APIs" to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.
ii. Enable quick and transparent integration with other e-Governance applications and systems.
iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.
iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.

v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.
ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.
iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.
iv. The Government organizations shall make sure that the Open APIs are stable and scalable.
v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.
vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.
vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.
viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.
ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.
x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.
xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

12.1.8 Annex-H (Internet of Things)

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).
IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. IETF IPv6 over Low power WPAN (6LoWPAN):

It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
6LoWPAN Frame Format
Fragmentation and Reassembly
Header Compression
Support for security mechanisms

e. **IETF "Routing Over Low power and Lossy (ROLL):**

IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)
RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)
RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**

It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. **Use Case/ Application Specific:**

i. **Industrial IoT (IIoT):** Object Modeling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modeling
- Structured Assurance Case Metamodel
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modeling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. **Consortia**

a. **Open Interconnect Consortium:**

OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. Industrial Internet Consortium:

It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

12.1.9 Annexure-H (Disaster Management)

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 - *Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)

8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

13 Annexure 2 (Control & Command Centre)

1. Operators Client Workstations for Command Control Center

S. No	Parameter	Minimum Specifications	Compliance (Yes/No)
1	Operating System (OS)	Windows 7 Pro, Ultimate or Enterprise, 64-bit	
2	CPU	Intel Core i7, 3.07 Ghz or Higher	
3	Memory	32 GB DDR3	
4	Graphics Card	Nvidia GeForce GT430 PCIe Nvidia GeForce GTX460 PCIe or faster.	
5	Network connection	Gigabit Ethernet (GigE) network connection required	
6	Monitor	Min 22 Inch or Higher	

2. Site Preparation and Minimum guideline for control room design

S.no	Parameters	Qty
1	Wall Size for Video Wall	Video-wall with Single Controller 55 inch
2	Workstations	As per BOM

3. **General Requirements and Specifications for Console System:** The following specifications detail the minimum requirements of the Console System. Bidders must respond on the enclosed chart. This allows for a point-by-point technical response stating compliance, taking exception or providing requested information. Bids submitted without this chart will be considered non-responsive.

MSI shall supply the following to obtain project level approval

a) Copy of ISO 9001:2008 Certification & ISO 14001:2004
b) Copy of Green guard certifications for full console.
c) Copy of FSC certification (Forest Stewardship Council) for Wood Components. Certificate for compliance towards sustainable forest initiative ensuring wood used is from sustainable forest harvesting.

The console(s) design shall be proven in service.

1) The consoles shall be of modular design, facilitating future equipment retrofits and full reconfigurations without major modification to structure or exterior elements.

2) The consoles shall have rigid independent frames.

3) Mechanical fasteners shall connect adjacent modules to maintain perfect alignment.

4) Depending upon the evolution of needs and technology, the construction shall provide easy and fast removal and installation of all equipment items.

5) The console frame shall have the Sit & stand actuator mechanisms incorporated into the structural frame and these actuator mechanisms will not be free standing on the floor.

6) The console frame shall have provisions for leveler legs to be incorporated into the frame. In addition, the frame will be pre designed to install optional anti-vibration dampers (upon request) or anchoring brackets for applications where vibration is a factor or for applications located in seismic zones.

7) The console frame structure shall have fully integrated cable management. The base structure will have a minimum of 2 lateral raceways; the transition from the base to the work surface will have a minimum of 2 vertical raceways; and the work surface will have a lateral raceway location depending on the Size of equipment being mounted in the console.

8) The cable raceways shall be continuous throughout the entire console layout thus allowing uninterrupted cable management.

9) The console design shall be acoustically acceptable and minimize noise reflection.

10) Consoles shall be properly finished to prevent glare and reflection.

11) No sharp edges shall be present that may lead to injury to the operators.

12) The color of the console shall be such that users can work for a long duration without eye strain or other stress.

13) The console finish shall be resistant to rubbing and liquids, impact-proof and easy to clean.

14) The surface of the work area shall be non-scratch able

15) The work surface should be smooth and level and take into consideration all accepted human factor criteria, including view, reach distances, keyboard height and knee well space. The work surface height shall be adjustable.

16) Full console Sit to stand height adjustment shall be available via an electric actuator. The top section of the console raises both the upper viewable equipment and the work surface together.

17) Detailed CAD (PDF format) drawings of console and equipment layouts for coordination of Site measurements, architectural, mechanical, and electrical project elements for each console type will be provided.

18) All Board Cladding (Laminates) must be 1MM & the Laminate supplier must be Green Guard Certified, Certificates of which must be provided on request

19) Renderings of consoles and room must be provided on request...

20) Pre-production review, to include a drawing submittal and component listing complete with samples of selected finish materials must be provided on request...

21) Samples of the following material components, which demonstrate workmanship, shall be provided upon request:

    a. Work surface sample.
    b. Sample panel construction and finish materials.

4. Modular Control Desk

Structure

a) Console System must be of modular design. The Console design shall address the functional, ergonomic and aesthetic requirements of the particular working environment while complying with accepted human factor design and ergonomic standards for viewing distance, angle, keyboard height, and knee space requirements.
b) Standard top height of modular control desk shall be 750 mm in sitting position and have to go till 1100 mm for Standing Position. The Console Table Top / Working Surface should be made in 12mm mm Solid Acrylic Panel (ASS) Cladded on 25mm MDF Board. Drawing is enclosed.
c) Size of modular control desk shall be as per drawing and it should have arrangement for placing of 2 workstations monitor for 2 Users on each control desk.
d) The Basic Structure should consist of Extruded AL Profiles (6063T6 grade) binded by Top & Bottom (min 2mm) MS Frames formed in such a way as to provide maximum buckling and

torsion resistance. The Front & Back Panels should be open able / removable (with Locks) made of laminated MDF Board in min thickness of 18mm. The front Shutter will be of Toughed Glass (min. 4mm Thick) cladded on 18 mm MDF and back shutter in 18 mm MDF Boards with Fan for Heat decapitation.

e) The Side Panels should be fixed type, made in 26mm MDF Board Cladded on 18mm MDF Board. All panels must be attached to the frame with concealed fasteners. Console access panels (Front & Rear Panels) must be removable without the use of tools. The Front panel should be ;

f) Positioned in such a way that there should be sufficient leg space (min of 400mm from the front edge of the Table Top).

g) All sheet metal / aluminum parts must be finished with electrostatic powder coating with average of min 80 microns over all surfaces.

h) The console frame shall have provisions for leveller legs to be incorporated into the frame.

5. Minimum Technical Specifications of video wall:

Video Wall Screen

Sr. No.	Parameter	Minimum Specifications
1	**Resolution**	Full high definition (1920 x 1080); 16:9 Widescreen
2	**Contrast ratio**	10000:01:00
3	**Brightness**	Minimum 500 nits and should be adjustable for lower or even higher brightness requirements
4	**Viewing angle**	178 degree/178 degree (H/V)
5	**Light Source Type**	• Laser light source with best in class Laser diodes. • Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen
	Dust Prevention	Should meet or exceed IP6X standard.
6	**Response time**	8ms
7	**Input**	HDMI
8	**Control**	• On Screen Display (OSD) • IR remote control

9	**Operations**	24 x 7 basis
10	**Power Supply**	Dual Redundant and Hot Swappable Power Supply. This should be built inside the cube for fail safe operation with cooling features.

6. Video Wall Controller

S.No.	Parameter	Minimum Specifications
1	**Controller**	Controller to control Video wall in a matrix as per requirement along with software
2	**Chassis**	19" Rack mount
3	**Processor**	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better
4	**Operating System**	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc
5	**RAM**	16 GB or more
6	**HDD**	500 GB (7200 RPM) or more
7	**Networking**	Dual-port Gigabit Ethernet Controller with RJ-45 ports
8	**RAID**	RAID 0, 1, 5, 10 support
9	**Power Supply**	(1+1) Redundant hot swappable
11	**Input/ Output support**	DVI/HDMI/USB/ LAN/ VGA/SATA port
12	**Accessories**	104 key Keyboard and Optical USB mouse
13	**USB Ports**	Minimum 4 USB Ports
14	**Redundancy support**	Power Supply, HDD, LAN port & Controller
15	**Scalability**	Display multiple source windows in any size, anywhere on the wall
16	**Control functions**	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate
17	**Inputs**	To connect to minimum 2 sources through HDMI

S.No.	Parameter	Minimum Specifications
18	**Output**	To connect to minimum 16 Displays through HDMI
19	**Operating Temperature**	10°C to 35°C, 80 % humidity
20	**Cable & Connections**	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units

7. Video Wall Management Software (VMS)

S.No.	Parameter	Minimum Specifications
1	**Display & Scaling**	Display multiple sources anywhere on display up to any size
2	**Input Management**	All input sources can be displayed on the video wall in freely resizable and movable windows
3	**Scenarios management**	Save and load desktop layouts from local or remote machines
4	**Layout Management**	Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	**Multi View Option**	Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	**Other features**	SMTP support
		Remote Control over LAN
		Alarm management
		Remote management
		Multiple concurrent client
		KVM support
7	**Cube Management**	Cube Health Monitoring
		Pop-Up Alert Service
		Graphical User Interface

8. Monitoring Workstations

S.No.	Parameter	Minimum Specifications
1	**Processor**	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2	**Chipset**	Latest series 64bit Chipset
3	**Motherboard**	**OEM** Motherboard
4	**RAM**	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC
5	**Graphics card**	Minimum Graphics card with 2 GB video memory (non- shared)
6	**HDD**	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
7	**Media Drive**	No CD / DVD Drive
8	**Network interface**	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9	**Audio**	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10	**Ports**	Minimum 6 USB ports (out of that 2 in front)
11	**Keyboard**	104 keys minimum OEM keyboard
12	**Mouse**	2 button optical scroll mouse (USB)
13	**PTZ joystick controller (with 2 of the workstations in ICMCC)**	• PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered
14	**Monitor**	22” TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified
15	**Certification**	Energy star 5.0/BEE star certified
16	**Operating System**	64 bit pre-loaded OS with recovery disc
17	**Security**	BIOS controlled electro-mechanical internal chassis lock for the

S.No.	Parameter	Minimum Specifications
		system.
18	**Antivirus feature**	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
19	**Power supply**	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.

9. IP Phone

Sr. No.	Parameter	Minimum Specifications
1	Display	2 line or more, Monochrome display for viewing features like messages, directory
2	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface
3	Speaker Phone	Yes
4	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5	VoIP Protocol	SIP V2
6	POE	IEEE 802.3af or better and AC Power Adpater (Option)
7	Supported Protocols	SNMP, DHCP, DNS
8	Codecs	G.711, G.722, G.729 including handset and speakerphone
9	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute
10	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer

11	Phonebook/Address book	Minimum 100 contacts
12	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13	Clock	Time and Date on display
14	Ringer	Selectable Ringer tone
15	Directory Access	LDAP standard directory

10. Desktops

S.No.	Item	Minimum Specifications
1	**Processor**	Intel Core i5-latest generation (3.0 Ghz) or higher OR Equivalent 64 bit x86 processor
2	**Memory**	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade
3	**Motherboard**	OEM Motherboard
4	**Hard Disk Drive**	Minimum 1TB SATA III Hard Disk @7200 RPM or higher
5	**Audio**	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6	**Network port**	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7	**Wireless Connectivity**	Wireless LAN - 802.11b/g/n/
8	**USB Ports**	Minimum 4 USB ports (out of that 2 must be in front)
9	**Display Port**	1 Display Port (HDMI/VGA) port
10	**Power supply**	Maximum Rating 250 Watts, 80 plus certified power supply
11	**Keyboard**	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
12	**Mouse**	Optical with USB interface (same make as desktop)
13	**Monitor**	Minimum 18.5” diagonal LED Monitor with 1366x768 or higher

S.No.	Item	Minimum Specifications
		resolution. (Same make as desktop). Must be TCO05 certified
14	**Operation System and Support**	Pre-loaded Windows 8.1 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. All Utilities and driver software, bundled in CD/DVD/Pen-drive media
15	**Certification for Desktop**	Energy Star 5.0 or above / BEE star certified
16	**Other pre-loaded software (open source/ free)**	Latest version of Libre-office, Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be preloaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

11. Laptops

Sr. No.	Item	Minimum Specifications
1	**Processor**	Latest generation Intel Core i5 (2 Ghz) or higher OR Equivalent 64 bit x86 processor
2	**Display**	Minimum 14" Diagonal TFT Widescreen with minimum 1366 x 768 resolution (16:9 ratio)
3	**Memory**	8 GB DDR3 RAM @ must be free for future upgrade
4	**Hard Disk Drive**	Minimum 500 GB SATA HDD @ 5400 rpm
5	**Ports**	3 USB Ports; 1- Gigabit LAN (RJ 45); 1- HDMI/Display port; 1- VGA; 1- headphone/Microphone
6	**Web Camera**	Built in web cam
7	**Wireless Connectivity**	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0
8	**Audio**	Built-in Speakers

Sr. No.	Item	Minimum Specifications
9	**Battery backup**	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours
10	**Keyboard and Mouse**	84 Keys Windows Compatible keyboard, Integrated Touch Pad.
11	**Operating System**	Pre-loaded Windows 8.1 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. All Utilities and driver software, bundled in CD/DVD/Pen-drive media
12	**Certification**	Energy Star 5.0 or above / BEE star certified
13	**Weight**	Laptop with battery (without DVD) should not weigh more than 2 Kg
14	**Accessories**	Laptop carrying Back-pack. It must be from same OEM as laptop
15	**Other pre-loaded software (open source/ free)**	Latest version of Libre-office, Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be preloaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.

12. Multi-Function Laser Printer

Sr. No.	Parameter	Minimum Specifications
1	**Technology**	Laser
2	**Monthly duty cycle/RMPV (pages)**	200,000/5K-20K
3	**Print speed – simplex (A4)**	Up to 41 ppm
4	**Scan speed – Black/Color simplex**	Up to 50/30 ipm
5	**Scan speed – Black/Color duplex**	Up to19/14 ipm
6	**Scan-to destinations**	Email, Network folder, USB

Sr. No.	Parameter	Minimum Specifications
7	**Processor (MHz)**	600
8	**Memory (MB)**	1,024
9	**Hard disk drive (HDD)/Capacity (GB)**	Yes/240
10	**Connectivity**	2 Hi-Speed USB 2.0; 1 Gigabit Ethernet 10/100/1000T network
11	**Print resolution – Max/Best print quality (dpi)**	Up to 1200x1200
12	**Input capacity – Std/Max (sheets)**	600/4,600
13	**Output size – Min/ Max (mm)**	76.2 x127/312x469.9
14	**Automatic duplex**	Yes
15	**Energy Efficiency**	BEE or Energy Star certified
16	**Control panel display**	20 m touchscreen

13. Laser Printer

Sr. No.	Parameter	Minimum Specifications
1	**Print speed black (normal, A4)**	Up to 25 ppm
2	**Print quality black (best)**	Up to 1200 x 1200 dpi
3	**Print technology**	Monochrome Laser
4	**Duty cycle (monthly, A4)**	Up to 15,000 pages
5	**Recommended monthly page**	volume 250 to 2000
6	**Standard memory**	Minimum 128 MB
7	**Processor speed**	Minimum 700 MHz
8	**Paper handling standard/input**	Up to 250-sheet input tray
9	**Paper handling standard/output**	Up to 150-sheet output bin
10	**Media sizes supported**	A4, A5, A6, B5, postcard

Sr. No.	Parameter	Minimum Specifications
11	**Media types supported**	Paper, transparencies, postcards, envelopes, labels
12	**Standard connectivity**	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity
13	**Duplex printing**	Automatic (standard)
14	**Compatible operating systems**	Microsoft Windows 7 Professional(64bit), Windows 8 Pro(64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux
15	**Power requirements:**	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);
16	**Power consumption during printing**	Less than 500W
17	**Energy Efficiency**	BEE or Energy Star certified
18	**Front operating Panel**	Graphical LCD display

14. Projector

Sr. No.	Item	Minimum Specifications
1	**Display Technology**	Poly-silicon TFT LCD
2	**Resolution**	HD 1080p
3	**Colors**	16.7 million Colors
4	**Brightness**	2500 or more ANSI lumens (in Normal Mode)
5	**Contrast Ratio**	2000:1 or more
6	**Video Input**	One computer (D-Sub, Standard 15 pin VGA connector), One S-Video, One HDMI
7	**Audio**	Internal speaker

Sr. No.	Item	Minimum Specifications
8	**Output ports**	External Computer Monitor port, audio ports
9	**Remote Operations**	Full function Infrared Remote Control
10	**Other features**	Auto source detect, Auto-synchronization, Keystone Correction

15. Online UPS

Sr. No.	Parameter	Minimum Specifications
1	**Capacity**	Adequate capacity to cover all above IT Components at respective location
2	**Output Wave Form**	Pure Sine wave
3	**Input Power Factor at Full Load**	>0.90
4	**Input**	Three Phase 3 Wire for over 5 KVA
5	**Input Voltage Range**	305-475VAC at Full Load
6	**Input Frequency**	50Hz +/- 3 Hz
7	**Output Voltage**	400V AC, Three Phase for over 5 KVA UPS
8	**Output Frequency**	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9	**Inverter efficiency**	>90%
10	**Over All AC-AC Efficiency**	>85%
11	**Technology**	• True Online Double Conversion • IGBT technology • PWM inverter switching technology
12	**UPS shutdown**	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short

Sr. No.	Parameter	Minimum Specifications
13	**Battery Backup**	60 minutes in full load
14	**Battery**	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
15	**Indicators & Metering**	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
16	**Audio Alarm**	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
17	**Cabinet**	Rack / Tower type, 75KW/ 150KW/ 200KW configurations
18	**Operating Temp**	0 to 40 degrees centigrade

16. Diesel Genset

Sr. No.	Item	Minimum Specifications
1	**General Specifications**	a) Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. b) KVA rating as per the requirement to provide the supply for KICCC
2	**Engine**	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002
3	**Fuel**	High Speed Diesel (HSD)

Sr. No.	Item	Minimum Specifications
5	**Alternator**	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
6	**AMF (Auto Main Failure) Panel**	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators: • Incoming and outgoing voltage • Current in all phases • Frequency • KVA and power factor • Time indication for hours/minutes of operation • Fuel Level in fuel tank, low fuel indication • Emergency Stop button • Auto/Manual/Test selector switch • MCCB/Circuit breaker for short-circuit and overload protection • Control Fuses • Earth Terminal • Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
7	**Acoustic Enclosure**	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangements etc.
8	**Fuel Tank Capacity**	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet

Sr. No.	Item	Minimum Specifications
		and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.

17. <u>ILLUSTRATIVE View Of Control Room</u>

18. ILLUSTRATIVE VIEW OF CONTROL DESK

19. IP CCTV camera for Control Room

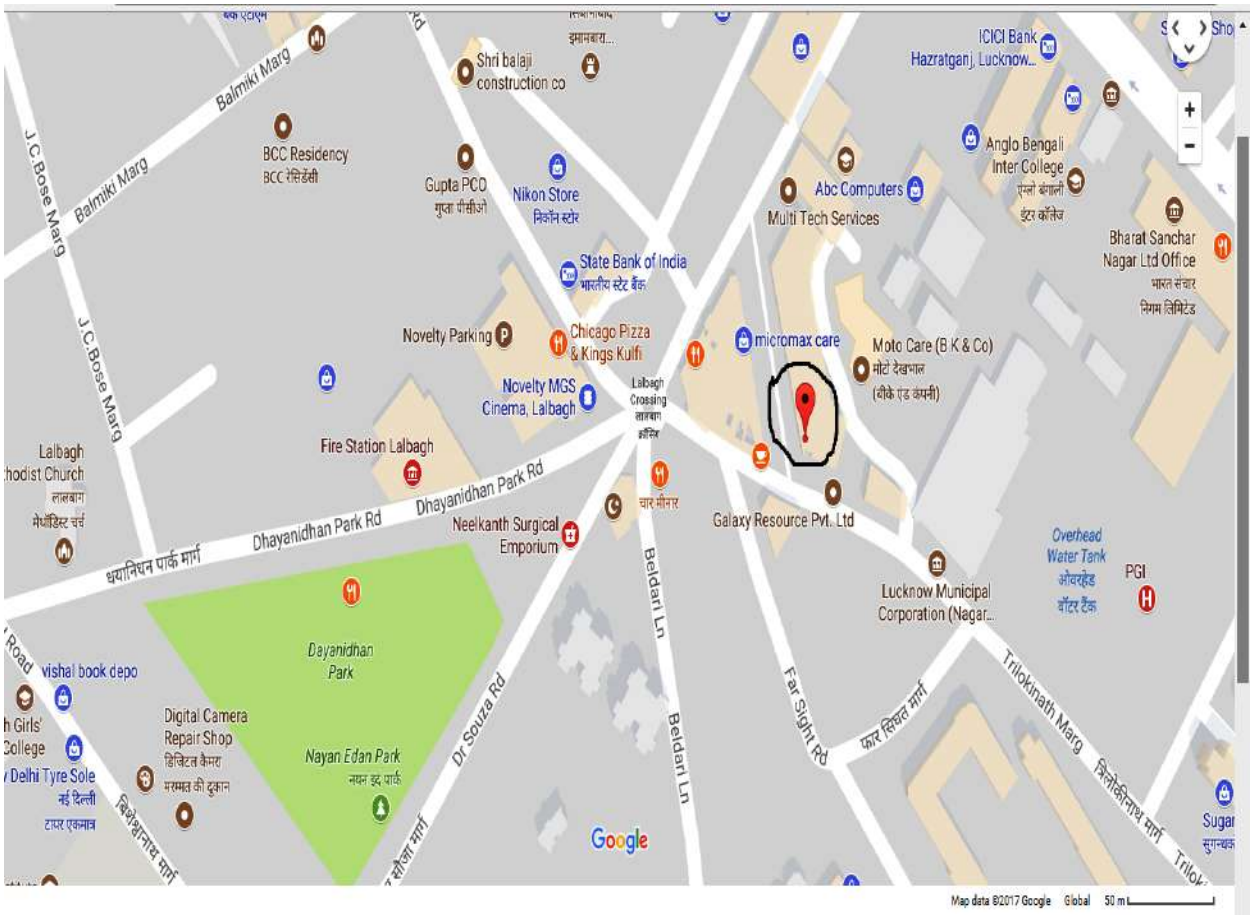
NO.	Camera Characteristics	Specification
1	Requirement Overview	IP Camera should be a high-definition, full-functioned video endpoint with industry-leading image quality and processing power. The camera is capable of resolutions up to 1920 x 1080 at 30 frames per second (fps) while optimizing network usage with either H.264 or MJPEG compression.
2	Sensor Type	1/3" progressive-scan CMOS with Vandal-Resistant Dome
3	Max Resolution	1920 x 1080 @ 30 FPS
4	Dynamic Range	100 dB
5	Lens/Iris	3-10 mm p-Iris , Remote focus and zoom
6	Minimum illumination	● Color mode: 0.16 lux ● Black-and-white mode: 0 lux with illuminator active
7	Remote Autofocus	Yes
8	Field of View	33° to 104° (horizontal) 19° to 56° (vertical) 39° to 121° (diagonal)
9	Camera Adjustment	Pan: 350° Tilt: 80° Rotate: 350°

NO.	Camera Characteristics	Specification
10	Privacy regions	The camera supports up to four user-defined privacy regions. Any video within a privacy region is masked in the video stream.
11	Audio I/O	Audio in x 1
12	Digital I/O	DI x 1, DO x 1
13	Number of streams	● Single-stream H.264 up to 1920 x 1080 at 30 frames per second (fps) ● Single-stream MJPEG up to 1920 x 1080 at 30 fps ● Dual-stream H.264 and MJPEG: ◦ Primary stream programmable up to 1920 x 1080 at 30 fps ◦ Secondary stream programmable up to 1024 x 576 at 15 fps
14	Day/Night	Automatic, manual, scheduled
15	Local Storage	Micro SD
16	Video Compression	H.264 & Motion JPEG
17	ONVIF	ONVIF
18	External Power	12V DC /24 VAC
19	Environmental Certification	IK10 and IP67-rated enclosure for outdoor mounting.
20	Power Consumption	Max 16 Watts at PoE
21	Operating Temperature	-20 to 50°C (-4 to 122°F) using PoE
22	Protocols	Dynamic Host Control Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Network Time Protocol (NTP), Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), Simple Mail Transfer Protocol (SMTP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), Transmission Control Protocol/Internet Protocol (TCP/IP), Secure Real-Time Transport Protocol (SRTP), Discovery Protocol, Bonjour, Simple Network Management Protocol (SNMP), and Secure Shell (SSH)
23	Camera Tamper	The camera should support tamper feature when any of the following events occur and persist for a designated period: • The IP camera view is changed • The IP camera view is blocked • The IP camera view is substantially out of focus
24	Quality of service (QoS)	Differentiated services code point (DSCP) marking and class of service (CoS) marking
25	Certifications Safety	UL60950-1 second edition CSA22.2-No.60950-1 IEC/EN60950-1 second edition IEC/EN60825

NO.	Camera Characteristics	Specification
26	Certifications EMC-Requirements	CISPR22 Class B ICES-003 EN50121-4 EN50155 EN50130-4 EN55022 EN55024 EN61000-3-2/-3-3 Class A VCCI Class B KN22 Class B KN24
27	OEM Criteria	All proposed Cameras should be from Single OEM and OEM should have Registration in India min from 10 Years

14 Annexure 3: Temporary Location for Command & Control Centre:

26°50'52.0"N 80°56'27.5"E



15 Annexure 4: Locations for Environmental Sensors

S.no	Location Name
1.	Chaudhary Charan Singh International Airport, Amausi, Lucknow
2.	Charbagh Railway Station, Lucknow
3.	Kaiserbagh Circle, Lucknow
4.	Begum Hazrat Mahal Park
5.	Polytechnic Circle

16 Annexure 5 Location for Variable Message Sign Boards:

S.no	Proposed Locations
1.	Charbagh Railway Station
2.	Hazratganj Circle
3.	Secunderabad Circle
4.	Gole Market Circle
5.	Nishatganj Circle
6.	IT Chauraha
7.	Munshipulia Circle
8.	Polytechnic Circle
9.	Kaiserbagh Circle
10.	Globe Park
11.	Samta Mulak Chowk
12.	Telibagh Circle
13.	Near SGPGI, Lucknow
14.	Alambagh Circle
15.	Bhootnath Circle
16.	Parivartan Chowk
17.	Dainik Jagran Circle
18.	Bangla Bazar Circle
19.	Tedi Pulia Circle
20.	Janeshawar Mishra Park

Note: The above locations are tentative in nature and the Master System Integrator has to closely work with LSCL before finalizing the locations.

17 Annexure 6 Functional & Technical Requirement shared by LMRC for Unified Metro Card

Concept note on "One City One Card"

One city one Card basically refers to interoperable Electronic Fare Management System. Besides the provision of an Automatic Fare Collection System, to serve the Lucknow Metro, there is a principally longer term objective to create an Interoperable Electronic Fare Management System. The primary function of the Interoperable Electronic Fare Management System is to permit users of public transport to travel seamlessly " door to door " through various types of transport networks. The principles of interoperability shall allow, as a minimum:

Intermodal Interoperability - where the one card held by the customer shall be accepted from one locality for use among different modes of travel such as LMRC, City Bus and UPSRTC. Seamless journeys require agreements between participating Service Providers, such as multiple transit operators, working to common rules and regulations to serve common goals regarding the integration of their fare collection systems, the use of common products, apportionment and settlement of revenue and costs, security and key management, system interfaces, etc. Central to the provision of such a scheme is the establishment of a proven framework incorporating an architectural, organizational and contractual basis, etc., by, which an Interoperable Electronic Fare Management System is to be realized.

One City One Card for the city of Lucknow

Lucknow Metro can act as the coordinating agency. The following shall be the system to be implemented /used for seamless integration:

1) The Ticket could be in the form of a smart card with a contactless chip inside. This card could be read at the Automatic Fare Collection Gate at LMRC and in the buses we could have stationary fixed readers at the gates of the buses or handheld readers with conductor of the bus. The card can be topped up with the amount while purchasing and gets initialized while it is used for the first time at any of the card reader either at the Metro or the Bus. The same concept can be extended to the Parking lots.

2) Distribution of the fare pro rata based on the journey performed by the passenger can be done through the Central Clearing House Scheme which shall be set up by LMRC and the fare earned by each transportation/non transportation agency can be transferred to their account once in a day based on the agreement between LMRC and concerned agency.

Technical Requirement

Lucknow Metro Rail Corporation is going to implement the Central Clearing House System along with Automatic Fare Collection (AFC) System, which is the part of the AFC System Contract of LMRC awarded to Consortium of M/s Datamatics and Mikroelektronika. With reference to One City One Card concept for Lucknow city, Electronic Media and their readers should be based on the same standards so that the same card can be operated at different locations among the transit/non transit operators. Other operators shall plan for the integration of their fare collection system to the CCHS implemented by Lucknow Metro Rail Corporation accordingly.

Specification of Card and SAM (Security Access Module)

Lucknow Metro Rail Corporation shall use readers in AFC system which supports both Type A (Mifare Desfire) based on the standard ISO 14443 and Type C (Sony Felica) smart cards however LMRC shall use Type A smart cards initially.

CCHS shall allow the Lucknow Metro Rail Corporation to manually transfer security keys and certificates to other agency or operators participating in the CCHS payment network to implement One City One Card concept. For this purpose a **Security Access Module (SAM)** is required which is a cryptographic Smart Media that provides security protection functions such as authentication and cryptogam for purse transaction. All SAM provided by LMRC shall meet the technical requirements for SAM as specified in **"Minimum Standards & Specification Document for Card and Devices"** released by UTIITSL.