Delhi Development Authority (DDA)

Digital Services

Request for Proposal

Selection of Agency for development and maintenance of "Computerized Management Systemfor Decision Support" and "On-line Public Services (including Grievances Redressal) System" (CMS) in DDA

Volume – II of III

Scope of Work

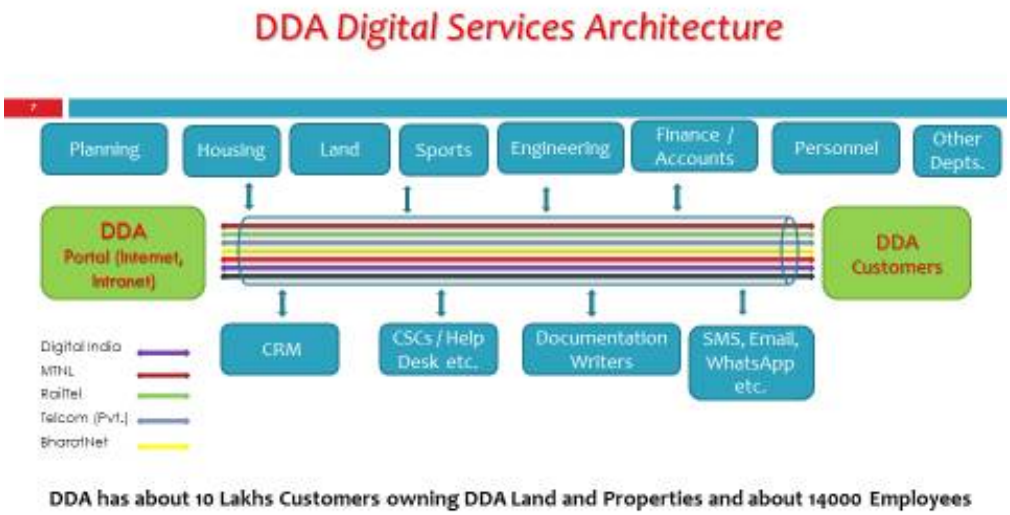
(Functional and Technical Requirements)

(Application Development, DC & DR Hardware & Network)

Contents

1 Scope of the Project/Work

DDA desires usher in Digital Service for based on the Services Architecture depicted in the Diagram given below.



DDA has about 10 Lakhs Customers owning DDA Land and Properties and about 14000 Employees

The Scope of the Project include, inter alia, the following Services: -

1. *Computerized Management System (IntraNet and Internet Portal) for Decision Support" and "On-line Public Services (including Grievances Redressal) (CMS)" Software Development, Roll-out and O&M;*
2. *ICT Infrastructure (Hardware, Software, IntraNet & Internet Networking, DC/DR) Installation and O&M;*
3. *Internet Services (Broadband, Leased line, etc.) and Data Centre Services;*
4. *Establishment of Help Desk, Call Centre and Facility Management System (FMS) and O&M;*
5. *Establishment of State-of-the-Art Record Rooms (50) and O&M/RFID related Technology based tags for Files management and O&M;*
6. *Data Digitization & Migration Services;*
7. *Establishment of Nagrik Suvidha Kendras and O&M;*
8. *Establishment of Mobile Van Nagrik Suvidha Kendra and O&M;*
9. *Establishment of Internet Information Kiosk;*
10. *Competency Development/ Capacity Building/Training of DDA Personnel; and*
11. *Capacity Building of DDA Stakeholders' (CSCs, Internet Kiosks Operators, RWAs, Document Writers, etc.).*

As a result, DDA desires to (i) to operationalize Integrated Workflow Automation for all Services, to strengthen "back-end Databases", (ii) ICT Infrastructures to support these Workflow Services, and (iii) to undertake capacity building / Competency Development of associated DDA Engineers/Officers/Officials etc., with the following features: -

1. *Web based Portal and to work, both on the Intranet and Internet - DDA IntraNet Portal and DDA InterNet Portal;*

2. *Appropriate bandwidth requirements so as to give a reasonable response time for Users on the Intranet/Internet;*
3. *Software Interface to be Intuitive and User-Friendly;*
4. *Centralized Database Server for data synchronization issues;*
5. *Application based 3-tier architecture to support large number of Users;*
6. *High Security "Database Vs. End - User "for any kind of reporting;*
7. *Queries to be optimized in Databases to avoid Locking and Performance Degradation Issues with large number of Users;*
8. *Seamlessly integration with the other existing Operational Software Applications and*
9. *Application of SMAC Technology (Social Networking, Mobile Technology, Data Analytics and Cloud Computing).*

As a result, DDA desires to (i) to operationalize Integrated Workflow Automation for all Services, to strengthen "back-end Databases", (ii) ICT Infrastructures to support these Workflow Services, and (iii) to undertake capacity building / Competency Development of associated DDA Engineers/Officers/Officials etc., with the following features: -

1. Web based Portal and to work, both on the Intranet and Internet - DDA IntraNet Portal and DDA InterNet Portal;
2. Appropriate bandwidth requirements so as to give a reasonable response time for Users on the Intranet/Internet;
3. Software Interface to be Intuitive and User-Friendly;
4. Centralized Database Server for data synchronization issues;
5. Application based 3-tier architecture to support large number of Users;
6. High Security "Database Vs. End - User "for any kind of reporting;
7. Queries to be optimized in Databases to avoid Locking and Performance Degradation Issues with large number of Users;
8. Seamlessly integration with the other existing Operational Software Applications and
9. Application of SMAC Technology (Social Networking, Mobile Technology, Data Analytics and Cloud Computing).
10. **Citizen-Centric System in view of their relationship with DDA: Aadhaar enabled Access, Public Dealing Module & Various related Software Modules shall be integrated so that relationships (lessee, license holder, member of any sports complex etc.) and services by DDA to a Citizen/Entity are accessible and provided through a Unique Account of the Citizen/Entity. These may include the updated particulars of all the relationships of that Citizen/Entity, latest status of application, communication of deficiency, if any, facility for uploading /down loading the documents, updated payment information and calculation of balance to be paid, if any, at any point of time and facility to make the Payment through Payment gateway.**
11. **Business Process Re-Engineering (BPR) – Mapping of Processes wherever possible, to make it Citizen-Centric. Reference may be made to the Business Process & Support Processes Study Report – computerisation of DDA (http://dda.org.in/tendernotices_docs/dec13/BUSINESS_PROCESS2260917.pdf).**
12. **Keeping of Electronic Depository of Property Rights (DEMAT) in Digital Locker Authority (http://www.dla.gov.in), constituted under the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker facilities) Rules, 2016.**
13. **DDA will ensure the procedure adopted is open and transparent, promotes healthy competition and is in accordance with both GOI and CVC Guidelines on the subject.**

The Scope also includes: -

1. Understanding of FRS and preparation of SRS and SDD; Undertaking BPR is a MUST;
2. Development, deployment and maintenance of a comprehensive Software Solution to meet all business processesas included (but not limited to) in this RFP and associated Annexures; including new processes emanating from BPR;
3. Finalization of templates for various forms, notices and other document required for manual forms and e-Services forms used for DDA;
4. Sizing & procurement, installation and commissioning of recommended IT infrastructure at Data Centre& Disaster Recovery Site and DDA's network size and design based on load tests, User Loads, scalability and future considerations.
5. Development, deployment and maintenance of web-portal (Internet and Intranet) which provides both informational and transactional facilities to Customers, meeting the Guidelines of Indian Government Websites (http://web.guidelines.gov.in), including Website Quality certification by STQC; **Portal will be in both in English and Hindi languages;**
6. Migration of Data from legacy applications and scanning of paper based records;
7. Creating central repository for all legacy data through integration and consolidation. Tasks involve Data consolidation, de-duplication and storage in form of single view of the citizen and their related information.
8. Setting up, Operations and maintenance of Helpdesk, Call Centre etc., to resolve customer queries regarding various processes, services of the department etc. as well as internal user queries regarding the Application trouble shooting etc.
9. Preparation of Training Plan, Training Material, Delivery of Training to Personnel of DDA in various Departments;

While providing a solution, the bidder shall follow the "Key Design Principles" as mentioned in RFP Volume 1. The Bidder is required to meet all the requirements of this RFP including the activities listed, timelines and deliverables mentioned in this RFP.

1.1 Geographical scope

The geographical scope of the project is limited to NCT, Delhi. Bidder is required to cover Head Quarters at Vikas Sadan, all zonal / circle offices of DDA including Sports Complexes **and SDM Offices**, etc.Illustrative details of the office locations are provided in the Annexure-1. Bidders shall conduct all application development related activities at DDA Head-Quarters (Vikas Sadan).

1.2 Application Software

The whole project is divided into two stages

a. Stage 1 – Customisation/Development and rollout of application
   i Phase I-roll out of Online Citizen Centric Services Including Public Grievances Redressal System for all Departments
   ii Phase II-roll out of all other services.
b. Stage 2 – Operations & Maintenance of solution post development and roll-out for 4 years + Warranty (1 Year) after stage 1

1.2.1 Stage 1: Customization /Development and rollout of application

In this phase, Bidder shall provide services for customization and development of the DDA-CMS (Computerised management system) Application. The following services shall be provided by Bidder:

1.2.1.1 Solution Design

1.2.1.1.1 System Study and Design

1. Study of existing applications with respect to its enhancement / integration /data migration and undertaking the same, if required. The details of existing applications along with their future plans is mentioned in Volume III of this RFP.
2. The System Integrator is required to adhere with the Functional Requirement Specification (FRS) as mentioned in the RFP.
3. The System Integrator should prepare the System and Software Requirements Specifications documents based on their understanding of FRS;
4. The bidder is also recommended **to carry out an independent system study** to thoroughly understand the function and operational process of DDA by -
    i Interacting with concerned officials
    ii Reviewing the existing systems if available
    iii Detailed study of requirements of CMS application components and solutions
    iv Understand Business process being carried out by the line department to deliver selected services.
    v Detailing various use cases scenario.
    vi Understanding / assessing data migration / digitization requirement and strategy;
    vii Understanding / assessing data inputs and outputs requirements;
    viii Collecting all input forms, registers and reports formats of DDA;
5. The System Integrator should prepare a detailed document on the implementation of CMSApplication with respect **to configuration, customization, extension and integration** as per the requirement of DDA. The System Integrator shall also prepare a change/reference document based on changes or deviations from the base version of the CMS Application with appropriate references to all the artefacts /documents provided by DDA.
6. As part of the System Study, the System Integrator shall be responsible for preparation of a comprehensive System Study document by studying the business processes and organization design of DDA.
7. The System Integrator shall perform the detailed assessment of the functional requirements and MIS requirements as part of the System Study document incorporating list of additional features that shall result in further improvement in the overall application performance for consideration of the DDA.
8. In case an existing application is being customized/configured to meet the needs of DDA, the System Integrator will provide a comparative report as part of System Study document, on the extent of functionality currently available in the application and the final FRS.
9. The System Integrator shall ensure that developed CMS application is fully compliant with the requirements and specifications provided in the RFP such as functional, non-functional and technical requirements. For ensuring this, the System Integrator shall prepare a Requirements Traceability Matrix;
10. The System Integrator shall create and maintain all project documents used in the project and shall provide access to DDAto review them. **The documents created by the System Integrator will be reviewed by PMU and approved by DDA**. Project documents include but are not limited to the following
    a. Detailed Project Plan
    b. Inception Report containing the project plan

c. Detailed System Study Report
d. List of services, Service Definitions, Service Levels
e. Updated/vetted FRS
f. SRS document (context analysis diagram (CAD) of manual processes and up to nth level CAD diagram of automated process)
g. Software Design Document (SDD) consisting of the following:
    i Software Development Document which will contain documentation pertaining to the development of each unit or module, including the code / software, approvals, etc.
    ii Security (Information Security Management System - ISMS) Plan
    iii Software operations and maintenance plan
h. HLD and LLD documents
i. ER diagrams and other data modelling documents.
j. Data dictionary and data definitions.
k. Application component design including component deployment views, control flows along with Hardware deployment based on Application Stack, Load test results & No of Users & future requirements.
l. GUI design (screen design, navigation, etc.) and all test plans
m. Requirements Traceability Matrix
n. Change Management and Capacity Building Plans.
o. SLA and Performance Monitoring Plan.
p. Business continuity / Disaster Recovery Plan
q. Third party integration plans
r. Version Control Mechanism document
s. Contingency Plan document containing emergency response procedures; backup arrangements, procedures, and responsibilities; and post-disaster recovery plans, procedures and responsibilities
t. Exit Management Plan

11. The System Integrator shall submit a list of deliverables that they shall submit based on the methodology they propose. The System Integrator shall prepare the formats/templates for each of the deliverables upfront based upon industry standards and the same will be approved by DDA prior to its use for deliverables.
12. Bidder must ensure that the system modules being developed are thoroughly documented with comprehensive manuals and adhere to standard methodologies in software development as per CMMi models. The documents including but not limited to are:
    a. Quality Assurance / Testing Plan documenting containing information on the software test environment to be used for independent testing, the test cases to be performed, and the overall testing schedule to ensure that the software developed will conform to the functional and technical requirements with traceability to those requirements. This includes methodology, schedule, resources, tools, procedures, environment definition, test cases, and software test results.
    b. Interface control document documenting the interface characteristics of one or more systems and documents agreements between interface owners. It contains information on both the physical and data element requirements that are necessary to make the transfer of information between systems feasible.

13. Preparation and maintenance of end-user documents including but not limited to user manuals. The manuals and documents etc. shall be in English and in soft and/or hard copy and equal to the number of the deliverables. Some of the user manuals are:
    i Operations Manual providing instructions for installing the application, troubleshooting, interpreting message logs, and FAQs (Frequently Asked Questions).
    ii Maintenance Manuals
    iii Administration Manual
    iv Security Manual
    v Applications and Web Portal Training Manual and others (if any) as per acceptable standards
    vi Systems Manual Detailing the data structure, table, forms and report structures.
    vii Trouble Shooting Guide/ Handbook for helpdesk which describes the various trouble shooting methods
14. All project documents are to be kept up-to-date during the course of the project. The System Integrator shall maintain a log of the internal review of all the deliverables submitted. Soft copy of logs shall be submitted to DDA on regular basis.
15. System Integrator shall upgrade and update DDA website
16. **The latest technology needs to be considered in proposing ICT infrastructure including but not limited to: virtualization, network convergence, Data Centre automation to achieve the optimum balance between cost and performance**.

1.2.1.1.2 Preparation of CMS Project Plan

1. The System Integrator shall prepare a comprehensive CMS implementation and deployment plan in consultation with DDA. This implementation document shall also comprise of :
    a. Capacity Building / Competency Development (Trainings) to be provided to the departmental officials at different stages of the project, procurement
    b. Deployment and commissioning of required software
2. Further, System Integrator will also prepare detailed work plan and estimate the timelines and resources required for configuration, customization, extension, integration, and commissioning of the CMS software as per DDA requirements. All the plans and frameworks prepared by System Integrator during the duration of the Contract **shall be required to seek approval** from DDA.

1.2.1.1.3 Preparation of CMS Application Design

Detailed Design documents shall include:

a. Technical Architecture Document (Application, Network, Hardware, and Security)
b. The available IT infrastructure available at DDA shall be a part of the document.
c. Gap infrastructure
d. High Level Design and Low Level Design.
e. Database architecture, including defining data structure, data dictionary as per standards (e-Governance Standards) defined by the Ministry of Electronics and Information Technology (MeitY), GoI/ DDA.

1.2.1.1.4 Sign off criteria

The solution design stage will be signed off on submission and subsequent approval of:

a. Detailed Project Plan
b. Detailed System Study Report
c. List of Services, Service Definitions, Service Levels
d. SRS document
e. HLD documents
f. LLD documents
g. CMS Application architecture documents.
h. ER diagrams and other data modelling documents.
i. Logical and Physical Database Design.
j. Data dictionary and data definitions.
k. Application flows and logic.
l. GUI design (screen design, navigation, etc.).
m. Requirements Traceability Matrix
n. Change Management and Capacity Building Plans.
o. Design of real time tools for monitoring e-Transaction volumes and for generating real time MIS
p. SLA and Performance Monitoring Plan.
q. Training and Knowledge Transfer Plans.
r. Issue Logs.

1.2.1.2 Software Development/Customization

1.2.1.2.1 Requirement on Adherence to Standards

CMS applications must be designed **following open standards**, to the extent feasible and in line with overall system requirements set out in this RFP, in order to provide for good inter-operability with multiple platforms and avoid any technology or technology provider lock-in.

1.2.1.2.2 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 projects of other departments / businesses in future, the solution should be built on Open Standards. The System Integrator shall ensure that the application developed is easily integrated with the existing applications. Every care shall be taken to ensure that the code does not build a dependency on any proprietary software. System Integrator must ensure that only Open Technology RDBMS is used.

1.2.1.2.3 CMS Application

The proposed application should confirm to the following requirements:-

a. The application should be developed on a Service Oriented Architecture (SOA) with centralized databases;
b. The application to be developed should support customization and configuration of application modules as per service requirements.

c. The application to be developed should confirm to inter-operability standards for e-Governance applications, be **Multi-tenant and Cloud-Ready** for having greater impact on the application delivery and productivity of DDA.

1.2.1.2.4 Application Architecture

1. It has been proposed that the applications designed and developed for the departments concerned must follow some 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.
2. Similarly 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.
3. An indicative 4-tier architecture (also referred to as multi-tier or N-tier architecture) has been proposed for the Application Solution. The entire processing should take place in n-tier architecture:
   a. Front-end software (client tier) - responsible for the presentation of information.
   b. Business Process / Service Layer
   c. Application Layer
   d. Database Layer
   e. Any other layer required as per the solution proposed
4. The application must be capable of supporting a minimum of 4500 internal users.
5. The application must be capable of supporting a minimum of
   a. 1000 concurrent internal users
   b. 5,000 concurrent external users at any time
   c. 15,000 concurrent external users for 10 days before "property purchase draw" closure deadline and 7days after declaration of results of each draw;
6. Application shall be modular in design, operations and implementation. This will give DDA, the flexibility to implement the whole system, or part of it as required;
7. Application shall provide interfaces and service to integrate harmoniously with external entities. This shall provide ability for applications and computers from different sources work seamlessly together on and across networks;
8. Application shall be integrated with communication channels like e-mail, payment Gateway, SMS gateways, WhatsApp Gateway (for mass communicating)etc. SMS Gateway will be utilized by the CMS application for sending service delivery related status updates to the citizens and processing USSD code requests from citizens;
9. Application shall use web services to implement service-oriented architecture.
10. Application shall have a browser based user interface supported by standard web browsers and shall not require installation of any specific client side software;
11. Application shall be independent of specific technology choices and therefore can operate on a variety of technology platforms;
12. System shall be developed using industry-recognized standard design methodologies;

13. System shall be designed so that business rules control access to data. Data is created and used by business processes. In computer applications, data must be created, used by, and managed by the application component that automates the business process.
14. Centralized data should be used wherever possible to assure data accuracy and simplify data management.
15. System shall adopt coding standards, in all languages, on all platforms. Coding standards make debugging and maintenance easier.
16. The code providing input and output to the user interface should be designed to provide input and output to as wide a range of interfaces as possible. This should include other applications as well as other types of user interfaces.
17. It should support Lightweight Directory Access Protocol (LDAP), in order to have integrated interoperability, security & manageability.

1.2.1.2.5 CMS Database

Each department will have access to its own data. However, services that span across departments shall also be supported. On top of core module and supporting middleware applications, there will be user access security layer supported by single sign-on (All application modules and third party support applications like Data Management System, Content Management System, Workflow, Portal, search engine etc.). The proposed application will use components for security, operational management, and communication to perform exception management, to authorize users to perform certain tasks, and to communicate with other services and applications. Other database requirements of the application are:

1. Application/Solution shall be able to archive transactional database records to prevent long term speed concerns.
2. Proposed database must support active-active architecture to ensure fail over support & high availability
3. Application shall feature functionality for efficient retrieval of archived data. The duration of archival and purging shall be specified by DDA generally the file will be archived on being marked as "closed".
4. Application shall design business rules for controlled access to data.
5. All data shall be maintained in a structured format in a Relational Database Management Systems (RDBMS) that clearly establishes the business entities and their linkages and dependencies with the rest
6. The data exchange formats shall comprehensively address all possible transactions and capture all transactional related information items.
7. Data exchange formats shall in human-readable format while addressing the constraints of machine interface required
8. Data exchange formats shall address the requirements of error check, data validation and audit related requirements. Vision of DDA is having an integrated automated system. Manual efforts to be minimized by adopting proper data validation mechanism.
9. The proposed application shall be capable of supporting standard databases.It is advisable to adopt an open non-proprietary standards that could be generic and extensible (to cover future requirements) in nature.

1.2.1.2.6 Enterprise Content management system

Enterprise Content management system (ECMS) is required to maintain the content on the web-portal. It should be possible to add content in form of Text, HTML, videos or Images on

the **DDA Website (DDA IntraNet and DDA Internet)**. Along with the facility to easily publish content on the website, CMS would also have facility to maintain access logs for security and accountability purpose.

1.2.1.2.7 CMS Functional Modules

The successful bidder shall be required to Design and develop the CMS Application as per the FRS and SRS finalized by all stakeholders. CMS aims at electronic delivery to all public. DDA has identified some high volume, high impact, citizen centric services for implementation on a priority. Later on, new services could be added depending on the requirements and the felt needs. The Identified services are listed in**Annexure – 34 and 34 A.**

1.2.1.2.8 Security

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

1. The system shall maintain accurate date and time.
2. System shall provide different and unique login IDs for all the users of the system and track all activities of all the logins and maintain audit trails of any changes made to the extent DDA deems necessary
3. The system shall identify and authenticate the user before providing him/her the access to IT systems. Identification is the process of distinguishing one user from all others. Identification techniques provide a means of gaining entry to DDA resources, such as applications. Mechanisms like use of multi factor authentication, digital certificates, challenge and responses, etc. shall be evaluated.
4. The system shall be able to grant specific access rights to each login or group of logins, as per the business requirement and policy of DDA. The application software shall be flexible enough to grant screen-based access to the users.
5. The application should have a centralized security management foundation that would enable delivery of application and data to internal and external users in a secure manner.
6. Avoid sending usernames and passwords unencrypted over the network.
7. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
8. The solution shall support advanced user authentication and data signing mechanisms including digital certificates.
9. The proposed solution should ensure that the user web access shall be through SSL (https) only for all level of communication for providing higher level of security.
10. User credentials shall be stored in an encrypted format
11. User credentials for external and internal users shall be stored in separate repositories
12. Ensure virus prevention with an automated update service on all critical systems for centrally managing the virus prevention
13. Using a central authentication service instead of host based password files
14. Using host integrity monitoring checks to protect the integrity of critical files and programs
15. 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.

16. The proposed solution should provide database security mechanism at core level of the database, so that the options and additions to the database confirm the security policy of the DDA without changing the application code
17. The proposed solution shall provide database encryption.
18. The database of the proposed solution should provide option for secured data storage for historic data changes for compliance and tracking the changes.
19. The proposed solution should be able to ensure the integrity of the system from accidental or malicious damage to data
20. The proposed solution should be able to generate a report on all "Authorization Failure" messages per user ID
21. The proposed solution should be able to differentiate between the systems of the DDA network and other external systems
22. Retention periods, archival policies and read-only restrictions must be strictly enforceable on all logs maintained in the system
23. The proposed solution should be able to monitor security and intrusions into the system and take necessary preventive and corrective actions.
24. The proposed solution must provide a security model that can be configured for enforcement of user rights
25. The proposed solution should be designed to provide for a well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
26. The proposed solution should have a Business Continuity Plan and a Disaster Recovery Plan prepared and implemented by the selected Bidder before commencement of the operations. Robust backup procedures to be established for the same.
27. Session Management shall allow various sessions to be managed across the business processes. It shall help in ensuring persistence across a transaction.
28. Exception Management shall take care of the various exceptions that might arise out of the system. These exceptions shall be captured and managed providing suitable abstraction to the user.
29. The proposed solution should support the below Integration security standards:
    - Authentication
    - Authorization
    - Encryption
    - Secure Conversation
    - Non-repudiation
    - XML Firewalls
    - Security standards support
    - WS-Security 1.0
    - WS-Trust 1.2
    - WS-Secure Conversations 1.2
    - WS-Basic Security Profile
30. The proposed solution should have a multi-layered detailed security system covering the overall solution needs having the following features:
    - Information and Incident Management Solution for complete DDA landscape;
    - Two factor authentication for all administrators i.e. system administrators, network administrators, database administrators.
    - Audit Log Analysis
31. The overarching requirement is the need to comply with ISO/IEC 27034 under the ISO/IEC 27001 standards of security. The Application Development Consortium Partner must be ISO27001 certified on Security Aspect and CMMi L5 on Maturity of Processes.

32. The application design and development should comply with OWASP top 10 principles;
33. The proposed solution will be monitored by periodic information security audits / assessments performed by or on behalf of the DDA. The scope of these audits / assessments may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, and program change controls. To the extent that the DDA deems it necessary to carry out a program of inspection and audit / assessment to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Selected Bidder shall provide the DDA's representatives access to its facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Selected Bidder must provide DDA access to various monitoring and performance measurement systems (both manual and automated). DDA has the right to get the monitoring and performance measurement systems (both manual and automated) audited / assessed without prior approval / notice to the Selected Bidder

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

i The security services used by application shall include: Identification, Authentication, Access Control, Administration and Audit and support for widely accepted industry standard protocols.

ii The application 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.

1.2.1.2.9 Scalability

One of the fundamental requirements of the proposed application is its scalability. The architecture should be proven to be horizontally and vertically scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance for at-least four years from the date of deployment. 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 application should be sized based on user load test & deployment shall be scalable to cater for the expansion of users of applications, processor, memory and the number of interfaces. The configuration proposed by Developer expected to have adequate upgrade capability. This should be achievable with minimum disruptions to Services, processes and Users.

b. Load Sharing - The load on the primary unit shall be shared with a secondary unit upon the primary unit reaching its capacity.
c. Solution shall support Performance Objectives / Optimization

d. Failover – Proposed configurations of equipment / devices shall have the capability to failover to a redundant or secondary unit upon failure of the primary unit.

1.2.1.2.10 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.

1.2.1.2.11 Support for PKI based Authentication and Authorization

The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000 and subsequent amendments, using the Digital Certificates issued by the Certifying Authorities (CA) such as MTNL,NIC or Other. The application/solution shall mandatorily support class III digital certificates. In particular, 2 factor authentication (login id & password and digital signature) shall be implemented by the selected Bidder for all officials/employees of the authority intending to use the solution.PKI Integration shall follow the latest interoperability standards issued by Controller of Certifying Authorities,Ministry of Electronics and Information Technology (MeitY), Government of India. The application shall also support digital signing and verification of data and forms.The supply of digital signature is not in the scope of work of this RFP and the same shall be procured separately by DDA..

1.2.1.2.12 Search

Search for different requirements and viewing corresponding details shall be provided in the solution. The search feature shall be linked to all modules of the application.

1.2.1.2.13 Web-portal

DDA has a dominant citizen focus; hence, in order to reach scale and enable e-service delivery, DDA's web-portal would provision information, interaction and transaction services for citizens / DDA customers and stakeholders. The core application will have two front-ends: One for the internal users of DDA available over the DDA intranet **(DDA IntraNet Portal)**and another for customers / stakeholders available over the internet (DDA Internet Portal).

1.2.1.2.14 Integration with Land Revenue department

The proposed application shall be capable of getting integrated with Land Revenue Department for obtaining 'Khasra/ Sizra' maps and land records including Information on "Mutation"

1.2.1.2.15 Integration with GIS / GSDL

The vendor will be required to manage the land records data (currently available with DDA in terms of alpha-numeric data) including the geo-referenced maps made available to the vendor. DDA will be responsible for procurement of all GIS data, cleaning / mosaicing / vectorisation / geo-referencing of all GIS data. Further, DDA will also procure the applications required by the vendor for managing and integrating the GIS data.

1.2.1.2.16 Third Party Software

Interface with design applications like AUTOCAD, REVIT or STAAD (but not limited to) used by various departments within DDA for integration with workflow and for other inputs. Files from these applications may need to be stored, forwarded, approved, etc. using the workflow management solution

1.2.1.2.17 Smart card readers and printers

The application shall have the functionality to allow use of smart card readers and printers. All DDA Sports complexes will issue "Membership Smart Cards" and thereby enable members to use and pay for using facilities through Smart Cards. Interface shall therefore be required with smart card printers as well as readers installed at access control points within Sports ComplexesBar Code Readers

Application shall have the functionality to generate bar codes and read them by using bar code scanners or manual input. All DDA office shall be equipped with bar code readers and generators for tracking movement of physical files and paper as detailed in the functional requirement specifications

1.2.1.2.18 Other external IT systems / applications of ministries & departments

Application shall support integration with external IT systems of ministries or government departments for obtaining various approvals and inputs.

1.2.1.2.19 Enterprise workflow management

Workflow management module (**based on workflow engine**) shall enable the workflows for various business processes. This shall include process tasks and routing. Workflow shall allow configuring various internal users into business processes for various kinds of approvals / rejections. For details refer to Annexures34and 34 A.

1.2.1.2.20 Facilitation centers & kiosks

The solution shall also provision customers to avail services through DDA facilitation centres and self-service kiosks(setup and management of kiosks ispart of scope of work of the current RFP). For example, facilitation centres can be utilized for financial information related to flats, shops or land allotted by DDA to the customer and using Kiosks customer can pay pending instalments, know payment details to be paid and get payment details history (when and how much payment has been done already). Kiosks can provide direct interface to the users to figure out property details without any intermediate layer, it can work on unique flat ID to fetch all relevant information to be available to customer at one place.

1.2.1.2.21 Enterprise management system (EMS)

EMS solutions are required to be provided consisting of the following components:

1. Application Monitoring System
    a. APM solution should ensure exceptional end-user experience and consistently high service levels that meet business objectives by monitoring all end-user transactions (Web and non-Web) 24x7 with low overhead. APM should accurately measure end-user transaction performance to prove IT is delivering against SLAs, business objectives and vendor commitments.
    b. Improve IT productivity and control costs by quickly and accurately diagnosing problems occurring deep within the application and infrastructure, pinpoint failures and speed problem resolution. Rapid problem identification and resolution often can be accomplished without impacting end users.

c. Assure high-value transactions receives the highest service levels by understanding problems in business context to identify critical transactions that may be at risk, prioritize problem resolution efforts, dispatch the right resources and fix the problems that impact revenue or key end users.

d. Application monitoring should map all transactions to the dependent infrastructure in real time for a single view of application health, business process flow and the entire transaction path to quickly triage issues

2. Service desk / Helpdesk Management System

a. System Integrator has to set up & manage a single unified helpdesk solution which should have flexibility of logging, viewing, updating and closing incident manually over phone, through intranet portal and also by e-mail. The Helpdesk must be accessible to other stakeholders via web interface.

b. The Helpdesk agent shall assign the tickets to most appropriate stakeholder based on category suggested by DDA for example the categories can be Application, Network & LAN, Laptop / Desktop & printer, Bandwidth, IT security etc

c. The proposed helpdesk solution must 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.

d. Each escalation policy must allow multiple escalation levels and notification to different personnel via window GUI/console.

e. The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

f. The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.

g. The proposed helpdesk solution must integrate with the Knowledge tools and CMDB and should be accessible from the login window.

h. Proposed helpdesk Solution should be ITIL v3 of 2007 Compliant / ITIL 2011 Compliant. L3 support person must be ITIL Certified Engineers.

i. Proposed helpdesk Solution should also have SLA tracking & Monitoring Capabilities & the solution should be able to monitor resources, independent of the platform & solution/service they are running. The proposed solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different KPIs like infrastructure (CPU utilization, disk space), response times, resolution times (eg. incident closed on 2 hours) performance and custom parameters of application and infrastructure at DDA.

j. The Solution should be able to monitor key performance characteristics of the resource (Application, RDBMS, Memory, Storage, Network etc.)

k. The Solution should have the mechanism to store the historical data for problem diagnosis, trend and analysis

l. The Solution should be able to send the reports through e-mail to predefined user with pre-defined interval

m. The Solution should trigger automated actions based on incoming events / alerts

n. The Solution should provide a Knowledge base to store history of useful incident resolution & have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance" it should also have Real-time visualization of service level targets, agreement compliance data, penalties and rewards

3. Remote management
4. Patch management
5. Security operations and Management
    a. The solution should provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Specifically, it should proactively secure access to data and applications located on system servers throughout the infrastructure.
    b. Security solution must allow controlling of access to all system resources including data files, devices, processes and audit files.
    c. The solution must provide support for IPv6
    d. Solution must intercept and verify every request to change user identity and maintain a reliable audit trail.
    e. Must provide centralized administration of user-ids and password management.
    f. Must provide a central directory of users, their business information, their accounts, and their access rights across the enterprise without requiring changes to end-systems.
    g. Must have APIs to enable additional user management operations over and above the default operating system account set-up.
    h. Must support enforcement of a centrally-defined security policy, e.g. for access rights, password lengths
    i. Must provide advanced Web support, to allow for smooth access and personalization of the user interface for each user. Once a user has been authenticated to the sign on system, access to all authorized Web applications and resources must be handled by this system.
6. SLA Advisor/Monitoring

Indicative SLA modules which are to be made available by the bidder on a web based system online for the DDA includes:

a. Project status
b. Solution (modules) availability
c. Quality of Service
d. Audit observations and the action taken
e. Training modules – Feedback, Number of sessions, trainees
f. Incidents report and Ticketing dashboard
g. Reporting

1.2.1.2.22 Payment and SMS Gateway

Integration of a payment gateway, SMS gateway and any other components required to meet the functional and Quality-of-Service requirements of the RFP is also within the scope of work of the System Integrator.

DDA will provision for the Payment Gateway, SMS gateway**/ WhatsApp Gateway**, and email gateway, and the bidder will be responsible for integrating these with the application.

Any applicable transaction charges for making electronic payments or using SMS based services shall however be payable by the citizen and need not be accounted for in the Total Contract value of this Project. Any transaction charges should be payable in Indian Rupees only.

The SMS gateway shall also support USSD Codes thereby enabling citizens to utilize service by mobile phones

1.2.1.2.23 High Level Design (HLD)

Once the SRS are approved, the System Integrator shall complete the High Level Designing and all HLD documents of all the functionalities, integration with existing application and external application. The System Integrator shall prepare the HLD and have it reviewed and approved by the DDA. DDA will sign off on the HLD documents based on the advice of ~~S~~PMU.

1.2.1.2.24 Detailed (Low Level) Design (LLD)

The LLD shall include product functionality, software architecture, decomposition description, data stores, design description, system design of all components and sub components including DFDs, configuration parameters, error codes, process description including flow charts, sequence diagrams. The LLD shall interpret the approved HLD to help application development and shall include detailed service descriptions and specifications, application logic (including "pseudo code") and UI design (screen design and navigation). The preparation of test cases will also be completed during this stage. The System Integrator shall have the design documents reviewed and approved by the DDA.

1.2.1.2.25 Compliance with Industry Standards

In addition to above, the proposed solution has to be based on and compliant with industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to design, development, security, installation, and testing. There are many standards that are summarised below. However, the list below is just for reference and is not to be treated as exhaustive.

a. Portal development W3C specifications
b. Information access/transfer protocols SOAP, HTTP/HTTPS
c. Content Management System - MeitY (GoI) guidelines
d. MeitY guidelines on use of Open Source Solutions / Open Technology Solutions
e. Photograph JPEG (minimum resolution of 640 x 480 pixels)
f. Scanned documents TIFF (Resolution of 600 X 600 dpi)
g. Biometric framework BioAPI 2.0 (ISO/IEC 19784-1:2005)
h. Latest HTML standards

1.2.1.2.26 Requirements change management

DDA does not intend to upgrade the version of the application during the contract period. The bidder should note that the system should be designed so that any rules, alerts, triggers, reports as required by the DDA should be catered to with no additional cost implications to the DDA. DDA would be required to issue circulars / orders periodically. The bidder is required to study the requirements and present the required changes in the system to the DDA and implement the changes in the system. The Bidder should define a formal process to manage the requirement changes as defined for illustration below:

a. Requirement traceability matrix
b. DDA shall be responsible to present the change requests initiated by user-groups and forward to the selected bidder.
c. The bidder should assess the need to implement the suggested changes, take necessary approvals to implement the suggested changes and present the change control note to the DDA for approvals.

d. Bidder shall maintain a change request log to keep track of the change requests. Each entry in the log shall contain a Change Request Number, a brief description of the change, the effect of the change, the status of the change request, and the key dates.
e. Bidder shall assess the effect of the change by performing impact analysis.
f. Bidder shall maintain the change request log with updated information and provide the same to DDA as and when desired.

1.2.1.2.27 Sign-off criteria

I. System Requirement Specification (SRS)
II. Traceability matrix including code v/s specification document and specification v/s code document.
III. Functional Requirement Specification (FRS) (if, updated)
IV. High Level Design (HLD) and Low Level Design (LLD)
V. Functional and non-functional testing reports
VI. Fully functional CMS Application
VII. User and Operational Manual for CMS Application

1.2.1.3 Testing and Development environment

1. Bidder should provide development environment license in the name of the DDA for the various tools used by Bidder during the development phase of respective solutions. These tools would typically include Application Development Framework / Environment for Custom Built and COTS/GOTSbased products, XML Schema Designer, PDF Designer, etc.
2. Biddershall provide all the hardware and all associated accessories (Racks, Cables, UPS, etc.) necessary for development testing and staging. DDA shall provide a facility to bidder for staging and conduct UAT for outside DDA offices. DDA shall also provide secured environment to store all staging servers brought by bidder in DDA campus for such activities.
3. The Bidder will be responsible for migration of staging environment to the DDA DC site as when it is ready
4. Application development shall be done at DDA Office. DDA will provide space and power supply to vendor.

1.2.1.4 Testing

Once the SRS is approved and design is started, the System Integrator shall prepare all necessary Test Plans (including test cases), i.e., plans for Acceptance Testing. Test cases for Initial and Final User Acceptance Testing shall be developed in collaboration with domain experts identified by DDA. Initial and Final User Acceptance Testing shall involve Test Case development, Unit Testing, Integration and System Testing, Functional testing of Application, Performance testing of the Application including measurement of all Service Levels as mentioned in this RFP. The Bidder will be responsible for providing the necessary development and testing environment and maintaining the related software and hardware for the Contract period. The System Integrator will submit the test plans and test result reports to the DDA for comprehensive verification and approval. The following sections explain the scope of each phase Bidder is expected to perform.

1. System test planning & testing
   a. Bidder shall plan out a series of different tests, each test having a different purpose, to verify that all system elements have been properly integrated and that the system

performs all its functions and satisfies all its non-functional requirements. Following tests need to be covered:

- Use Case Design
- Test Script Development for Central system functional testing
- High Volume performance testing
- Failure mode and anomalous behaviour tests
- Introductory, silent running & system readiness tests

b. The inputs for this phase consist of the SRS and the initial system test plans whereas the outputs consist of system test plan and test results.

c. As part of system test planning, Bidder shall identify features that shall be tested

d. On successful completion of the Integration testing, Bidder shall carry out the actual system testing as per the system test plan.

e. Bidder shall ensure that system testing is carried out by an independent team other than the development team. Bidder shall setup a separate test environment with test database to carry out system testing.

f. As part of the system testing, Bidder shall carry out Performance testing of the application to ensure that the application meets the performance requirements identified in the SRS.

g. Bidder shall maintain the system test plan and test results with defect statistics and provide the same to DDA.

2. User acceptance testing

a. Bidder shall prepare a plan to coordinate the User Acceptance activity.

b. Bidder shall prepare a software release note that contains stepwise instructions for DDA on how to install the software. The instructions shall include information on creating the directory structures, installing source and executables, loading data needed for installation and so on.

c. The primary responsibility for acceptance testing lies with the end user group and DDA shall coordinate with the Bidder to ensure necessary support is available to the end user group.

d. End user group shall review the test cases / scenarios to ensure that the defined acceptance criteria are validated during the acceptance testing.

e. Bidder shall provide the necessary infrastructure like servers, storage, , database licenses, development and run-time licenses for solutions proposed, etc. for the UAT environment. Bidder shall set up the test environment along with installation of the software and test data creation. Bidder shall be responsible for ensuring appropriate OS, Database versions and patches are installed on the respective servers in this environment. Any problems encountered during the installation shall be documented by Bidder and the installation manual shall be updated accordingly.

f. Bidder shall provide support to document the User Acceptance Test Results along with Defects Statistics. Bidder shall ensure that defects found are corrected and is retested by the end user group.

g. On successful completion of User Acceptance Testing, Bidder shall obtain a formal acceptance sign-off from DDA.

3. Integration testing

a. Bidder shall conduct integration test/ dry run with all DDA HQ and zonal offices, before 'roll-out' for each service/ process or group of process that are ready. Bidder is also required to prepare detailed plan for the same.

b. Bidder shall coordinate with DDA to resolve any problems encountered during and after rollout. All post implementation issues shall be documented and the necessary fixes / resolutions shall be implemented by bidder.

c. Bidder shall ensure necessary support is provided to resolve defects. Bidder shall document the defects / bugs encountered during this phase as well as document the resolution of the same. Bidder shall also prepare and maintain a database of Consolidated List of Common Errors & their Resolution.

4. Bidder shall conduct integration test/ dry run with all DDA HQ and zonal offices, before 'roll-out' for each service/ process or group of process that are ready. Bidder is also required to prepare detailed plan for the same.
5. Bidder shall coordinate with DDA to resolve any problems encountered during and after rollout. All post implementation issues shall be documented and the necessary fixes / resolutions shall be implemented by bidder.
6. Bidder shall ensure necessary support is provided to resolve defects. Bidder shall document the defects / bugs encountered during this phase as well as document the resolution of the same. Bidder shall also prepare and maintain a database of Consolidated List of Common Errors & their Resolution.

1.2.1.5 IT Security infrastructure

1. The bidder should recommend and procurenecessary devices to capture system and application logs from servers, network equipment and other hardware. The PCs will be provided by the hardware vendor on behalf of DDA.
2. The Bidder should secure application against unauthorized access from internal or external sources.
3. The Bidder should also provide a mechanism for tracking the security incidents and identifying patterns if any. The tracking mechanism should, 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
4. The Bidder should provide intrusion management services to protect DDA's resources from internal and external threats.
5. The bidder should provide sizing and specificationsfor procuring the necessary hardware/ software required for efficient intrusion management.
6. No products supplied under the RFP should be end of life during the project period. Bidder would have to upgrade to latest version during the project period.

1.2.1.6 Infrastructure Design Requirements

1. Bidder shall independently design thesoftware, server &storage infrastructure and accessories as required for the solutions that shall be deployed at the DC and the DR sites.
2. Bidder has to procure and install the required server & storage infrastructure at DC/DR and shall necessarily consist of components like but not limited to:
   a. Servers
   b. Data Replication Tool between DC & DR
   c. SAN Storage Array
   d. SAN Switch
   e. Tape Library
   f. Backup software

g. Infrastructure for NOC

Bidder would have to clearly state the requirement based on load testing & future requirements such as scalability etc.

3. Bidder shall include all the components (other than mentioned above) that are required to make the solution complete.
4. Tape library
   a. Bidder should provide the tape library requirement as a backup device for copying the data on to a removable media.
   b. Bidder should provide the tape library based on estimated data size and considering a full backup window of 4 hours. The number of tape drives should be provided accordingly.

1.2.1.7 STQC Certification

The System Integrator will be responsible for engaging STQC to conduct the assessment / review for the system before "Go Live" and shall also bear all the costs for the same. The PMU and DDA shall have the right to audit and inspect all the procedures and systems relating to the provisioning of the services. If there is any change / addition in the application's functionality then the System Integrator will have to obtain the STQC Certification for the changes / additions. Successful completion of Application Audit. Application audit will include:

a. Functionality audit that will map the functionality delivered to the FRS agreed upon during development phase.
b. Identify the nature and type of transactions being processed by the application systems.
c. Determine systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc.
d. Review of database structure including:
   i Classification of data in terms of sensitivity & levels of access
   ii Security measures over database installation, password policies and user roles and privileges
   iii Access control on database objects – tables, views, triggers, synonyms, etc.
   iv Database restoration and recoverability
   v Audit trails configuration and monitoring process
   vi Network connections to database
e. Review of Network and Website will include:
   i Penetration and vulnerability testing
   ii Security exposures to internal and external stakeholders
f. Definition and Implementation of Security Policies and Controls will include:
   i Define and implement backup process, including schedule, storage, archival and decommissioning of media
   ii Define physical access controls review (over DC and other critical area)
   iii Define IT Change Management process, Incident Management process – covering identification, response, escalation mechanisms

iv Define and implement Anti-virus (malware) controls – patching, virus definition file update

g. Sign-off criteria
   i Sign off from DDA
   ii STQC Certification

1.2.1.8 Implementation and roll out

Bidder, in coordination with DDA, shall set up the production environment, installation of the application in the production environment, creation of application database, creation of application user profiles, loading the legacy data, etc. Services including, but not limited to, the following should be provided:

a. Planning and Scheduling for installation and commissioning of hardware and equipment for production and testing environment.
b. Installation and commissioning of hardware and equipment for production and testing environment.
c. Requirement validation
d. Preparation of core database design
e. Software development, customization, roll-out for applications
f. Request & coordination with DDA for integration of network (WAN, LAN and Internet)
g. Configuration and tuning of all the installed equipment and software for production and testing environment.
h. Integration and testing of installed systems / subsystems / equipment / Software.
i. Co-ordination and troubleshooting with existing vendors to ensure that the solution is properly configured.
j. Planning and Implementation of migration of legacy data from existing database to the target database.
k. Ensure that all the solutions are properly rolled out

Bidder should plan rollout of solutions in phases. The indicative phase-wise rollout plan is mentioned in the RFP. The bidder is required to coordinate the application roll-out at all DDA offices. Also, the bidder is required to support the technical implementation and rollout issues faced by the respective locations. Acceptance of system shall only be given when solution roll-out is complete at DDA head-quarters, all zonal / circle offices. DDA shall provide infrastructure comprising:

- IT infrastructure: Computer and Network
- Physical Infrastructure: Space, power and manpower for training

1.2.1.9 UAT and Go-Live

Bidder will assist in successful completion of User Acceptance Testing (UAT) and audit of the system on the completion of the roll out of CMS for each phase and will submit a Go-Live Report for each phase.The bidder shall integrate the hardware including the LAN, system software and application software and commission the whole project. The DDA/PMU shall conduct User Acceptance Testing on receipt of intimation of commission of the whole project from the bidder. Only after the acceptance of UAT reports by DDA, the entire infrastructure

(including CMS application) would be deemed to have been commissioned. System Integrator should provide following documents to the DDA:

a. Installation Manuals
b. User manual (Role wise)
c. Access Control Policy
d. Incident Management Policy
e. Change management plan development
f. Transferring the ownership of all software developed/ customized/ configured/ procured.
g. All licenses & support related documents should be in the name of DDA.

Sign-off Deliverables

a. Go-Live report (Go-live criteria has been defined in RFP Volume I, Section 9.9)
b. Roll Out Completion Report
c. UAT Report signed off from concerned Officer
d. Source code of the solution

1.2.1.10 Application Support for Rollout of services

The System Integrator is expected to provide technical and operational support till the new system goes live and during the four-year Operation and maintenance phase. The System Integrator is required to provide minimum resource persons as mentioned in the Annexure 33. An indicative list of activities to be performed by various resources is also specified in the same annexure.

An indicative list of activities to be performed by the deployed resources for existing system support is:

a. Project Manager shall be the SPoC(Single Point of Contact)to the DDA/PMU/ Department for the implementation of the project.
b. The other staff shall function based on the scope of work of the RFP and contract signed between System Integrator and DDA.
c. If required System Integrator shall provide additional manpower to complete the work/task within timelines. While during the tenure of the project the DDA can instruct System Integrator to change the manpower at any location as per the requirements of DDA/Department.
d. System Integrator will provide the list of actual deployed manpower on monthly basis.
e. System Integrator will ensure that all the resources deployed at any location are easily approachable over mobile phones. System Integrator will provide the contact details of the manpower at the time of commencement of operations. System Integrator will also ensure that the proposed resources will not be changed during project implementation without explicit approval of the DDA.
f. The DDA reserves the right to evaluate the performance of the resource persons deployed on the project by System Integrator and ask for a suitable replacement in case of unsatisfactory performance by any of the resource persons deployed to support the project.

1.2.1.11 Data Digitization

Document digitization is the process of converting manual documents into digital formats. This is of paramount importance to the CMS project. In order to enable the selected departments to work on designed electronic workflow system of CMS, the concerned officials may require referring old records. Therefore, as per the requirement old manual records should be digitized. The data of all the services of the identified department should be ported in to the CMS application.FRS (Annexure-34) has further details on Document Management Solution (DMS) and shall be referred and adhered to.

The Benefits of Data Digitization:

- Easy and structured storage of data
- Avoids duplication of data
- Quick and easy retrieval
- Easy access
- Easy transportation
- Easy to share
- Makes data compatible with all modes of digital data transfer and data migration
- Perpetual preservation of all your vulnerable physical documents
- Portability of data between integrated applications

1.2.1.11.1 Guidelines and instruction for data digitization

1. System Integrator shall digitise all historical data as recommended by DDA.
2. System Integrator shall formulate the Data Digitisation Strategy which will also include internal quality assurance mechanism. This will be reviewed and signed–off by DDAprior to commencement of data digitisation.
3. System Integrator shall incorporate all comments and suggestions of DDA(FRS – DMS – Annexure-34 and also existing Scanning Policy)in the Data Digitisation Strategy.
4. The Bidder will provide interface in the application to capture legacy data, this interface should have inbuilt validation check like date format, field value, address etc. It should have provision to enter record in back date also. The software should have provision to data consolidation;
5. System Integrator shall perform pilot data digitisation exercise to validate the conversion programs.
6. System Integrator shall ensure complete data cleaning and validation for all data digitised and loaded on to CMS Application.
7. Concerned departments will validate the digitized data before System Integrator will upload the same to the production environment.
8. System Integrator shall generate appropriate control reports before and after digitisation to ensure accuracy and completeness of the data.
9. System Integrator shall conduct the acceptance testing and verify the completeness and accuracy of the data Digitised to CMS Application.
10. DDA and PMU may, at its will, verify the test results provided by System Integrator.
11. System Integrator shall provide resources for data digitisation on a monthly basis. Estimated resources required for data digitisation is detailed in Annexur-33. However, the System Integrator is free to recommend alternate resource requirement depending upon the solution proposed.
12. Quality Check-The bidder should ensure 98% data accuracy. Random checking will be conducted by the officer/agency appointed by the data digitization committee.

13. Bidder should take good care of all Government records and will be responsible for security of the record from time of receipt to time of delivery. Penalty for per record will be charged against the loss or damage of record.
14. The bidder should not accept illegible record. Non-readable record at the time of returning of the data will be considered as damaged record.

1.2.1.11.2 Scope for Data Digitization

The scope of data digitization should be based on Services identified, current status of digitization and Quality of existing records. The digitization and migration would include:

- Profiling of Legacy Data
- Conversion of Legacy Data
- Verification of Digitized Data

Data profiling will be taken up as per below mentioned method:

- **Column Profiling:** Analysing the values in each column or field of source data
- **Dependency Profiling:**analysing data across rows, comparing values in every column with values in every other column and infer all dependency relationships that exist between attributes within each table.
- **Redundancy Profiling:** Compares data between tables of the same or different data sources for overlapping or identical sets of values.

Once the legacy data is converted to target data, the source and target data needs to be verified to ensure that the target data (in new format) is the same as the source data. The Verification of target data should be done by team of DDA staff nominated by concerned departmental office. The data verification team would recommend/ certify the successful completion of digitization and migration of legacy data for CMS application as per desired standards. The certificate of satisfaction must contain the number of records digitized/ migrated, name of database, remarks and other relevant information.

Data digitisation services should provide for provision for scanning upto A0 page should be provided. 99% of the pages are in a4 or legal size.

Post data entry, a 2 stage data quality check needs to be carried out on the following lines.

- 10% data check by the Departmental officer at site.
- 10% data check by the Departmental official at Vikas Sadan/Vikas Minar/Offices

The data entry vendor will be penalized (should be mentioned in the contract) for poor quality of data entry(as defined in SLA in volume III of RFP).

The following data will be provided by DDA for digitization:

- ~ 15 lakhs files with approximately 100 pages per file (No. of files may likely to vary)
- Pages could be a mix of A4/ Legal size
- 50% handwritten/ 50% typed

- pages are written in English
- Upto 200 characters of metadataentry per file

1.2.1.11.3 Data Migration

Migrating the data from the other systems/manual operations to the new system will include collection and migration of user data, collection and migration of master data, closing or migration of open transactions, collection and migration of documentary information, and migration of data from the legacy systems. Integration of existing data with new digitized data is to be undertaken with appropriate data quality checks.

The System Integrator shall perform the data migration from existing systems (If any) to the new system. The Data migration task shall be preceded by an appropriate data migration need assessment including data Quality Assessment. Tasks involve data consolidation, de-duplication and storage in form of single view of the citizen.

Sign off criteria:

- Data Digitisation Strategy Document
- Approval by DDA / PMU on successful digitisation of data

1.2.1.12 System Software Licenses

1. All the system software licenses shall be proposed and supplied by the Bidder along with Detailed Bill of Material in the Financial proposal & shall be genuine, perpetual, full use and should provide upgrades, patches, fixes, security patches and updates directly from the OEM. All the licenses(vendor must consider existing DDA user base and estimated increase during the project duration) and support (updates, patches, bug fixes, etc.) should be in the name of DDA;
2. The software licenses shall not be restricted based on location/ hardware and DDA shall have the flexibility to use the software licenses for other requirements if required;
3. All the licenses and support (updates, patches, bug fixes, etc.) should be in the name of DDA. System Integrator shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance by DDA. The warranty should cover all materials, licenses, services, and support for both hardware and software. System Integrator shall administer warranties with serial number and warranty period. System Integrator shall transfer all the warranties to the DDA at no additional charge at the time of termination of the project. All warranty documentation (no expiry) will be delivered to Department.
4. System Integrator shall review the licenses requirements with the PMU and Engineer In-charge of the Project.

1.2.1.13 Capacity building and training

Bidders shall undertake capacity building exercise .Capacity building will include the following but not restricted to

1. Imparting training on new IT application developed. Such trainings and skills will be imparted to all levels of DDA employees involved in the processes pertaining to the selected services/Process
2. Preparing the detailed training plan, training manuals and training materials i.e. Prepare and organize training programs to facilitate the user departments in the efficient usage

of the new system training will be provided to department's employees whose Information & services will be provided through CMS Application.

3. Imparting training to the personnel identified by DDA, in the operation of the application software, generation of MIS reports and maintenance of user Logins etc. at various office locations.
4. Bidder shall prepare interactive Online Training Module for the application. Interactive modules should be available in English language. It should be accessible to all the users based on their requirement on the intranet.
5. Bidder shall ensure necessary data creation to conduct end user training
6. The training sessions and workshops should comprise of presentations, demonstrations and hands-on mandatorily for the application modules
7. For all these training programmes, the System Integrator has to provide necessary course material, user manuals, system admin, manuals etc. to the trainees. The language of different types of trainings to be provided to the identified staff under CMS project would be English.
8. The proposed training module is expected to help the department functionary to undertake their revised roles and responsibilities with ease and without any difficulty and apprehension. The training modules will impart the required skill set and capacity for performance of defined roles and responsibilities. Further, reinforcement training will be provided as per the requirement as assessed after the training program is over. The following training modules are proposed to be undertaken across the departmental hierarchy:
    a. CMS Orientation/Sensitization training: The orientation program is expected to generate awareness about the CMS project across all levels of the departmental hierarchy. The program outlines to DDA and communicate the objective of the project to all the stakeholders. An introduction to incorporation of technology as an enabler and supportive in discharging roles and responsibilities of government official will be integrated in CMS orientation program. Training material: A book on Orientation to be provided by the System Integrator in English language and System Integrator may provide orientation manual in English only. (Soft Copy) to the Department.
    b. CMS Application Training: This training is proposed to bring in detailed understanding of revised process and procedure for the selected services covered under the project and should include
        i Process/Activity Training-The Process training will detail out the step-by-step of the service process to concerned actors so as to acquaint them and help them understand the revised process. The training will detail out the roles and responsibilities of the concerned actors in the revised process. Training material: A book on Process Training to be provided by the System Integrator in English language.
        ii Activity Training: Activity training is envisaged to prepare the ground functionary based on the expected roles and activities to be performed in fulfilling the defined roles and duties. Activity training will first enlist down all the roles entrusted and then break the roles in terms of activity to be performed to meet the role. Once established the activity will be explained in terms of revised process of service and integrate the same with the computer use. Also, at the same time in-depth clarity will be provided to the trainee about the other associated factors like service levels, auto escalation and monitoring & control aspect of the CMS Application. Training material: A book on Activity Training to be provided by the System Integrator.

iii CMS Module Training: The CMS application Training is envisaged training compulsory for government official cutting across departmental hierarchy. The training is proposed to acquaint and train the work force with the various modules of CMS application by the use of computer. The training will be initiated through class room training through screen shots of the software for concerned actors and then followed by detailed training over the CMS application over computer. Training material: A book on CMS Application Training to be provided by the System Integrator in English language.

9. The Bidder will be responsible for collecting the feedback from all the trainees for each session. The feedback form should be prepared and shared with the DDA prior to the trainings. The feedback forms should include feedback on the coverage, quality of presentation, demonstration and hands-on sessions, expertise of the instructor and additional suggestions.
10. The bidder will be responsible for establishing a scoring system and should ensure a rating of at least 75% or above on the overall sessions else additional trainings will required or the DDA reserves the right to invoke penalty.
11. The bidder is responsible for making the feedback available for the DDA to review and track the progress through a web based online system.
12. Training shall encompass the knowledge of basic functionalities of CMS Application, Guidelines and other backend processes.
13. Training shall also be provided for teaching the basic trouble shooting activities in case of problems.
14. Trainings shall be provided to all the new employees as and when joining the department.
15. Trainings will be conducted in DDA designated training centres at Delhi, depending upon the number of trainees and availability of training centre.
16. Indicative number of trainees is 4000-5000, with a batch size of maximum 15 participants and an estimate of three trainings per user. Training of Users shall be in both English and Hindi languages;
17. The Bidder will be responsible for providing the necessary training environment and maintaining the related software for the Contract period. However, DDA shall provide all the requisite training related infrastructure and facilities.

1.2.1.14 Manpower Requirements

1. The project would require minimum provisioning of dedicated manpower at DDA Offices as detailed in Annexure 33. The System Integrator shall estimate the resourcing requirement and may quote for resource requirement and above the minimum requirement.
2. The System Integrator would be required to position resources to provide technical support at each of the office during the roll out period. This would be essential to ensure sufficient handholding is provided to department personnel in the various offices to manage the system after the end of System Integrator's Contract Period.
3. The Technical support resources would be required to work closely with the Project Manager and PMU in ensuring adherence to the project timelines.
4. The System Integrator should ensure that the roster schedule of all deployed manpower for each day at the required locations has been communicated in advance to DDA. No change to the deployed staff shall be done by the System Integrator without written approval from the DDA.

5. Adherence to all laws pertaining to personnel, labour laws, etc. for any manpower deployed by the System Integrator on this Project shall be the responsibility of the System Integrator
6. The System Integrator would issue Identity cards to each of the staff members deployed at the sites
7. The System Integrator will maintain adequate leave reserve for the staff, so that the work in the respective offices remains unaffected in all cases.

1.2.1.15 Business Continuity Planning

The selected Bidder is expected to develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for the operations carried out by the selected Bidder. An indicative list of activities to be performed by the selected Bidder is mentioned below:

a. Designing and implementing adequate data backup, business continuity and restoration procedures for the CMS application data (including but not limited to the database, attachments and all other data elements created in and generated by the system and users)
b. Ensuring that there is no single point of failure and adequate level of redundancy is built in to meet the uptime and other requirements of this RFP. While building redundancies, it should be ensured that failure of a single component of communication link does not result in failure of primary as well as secondary connectivity. Bidder has to coordinate with the Data Center & DR Hosting / Cloud service provider for mock DR drills, Data Replication & Restoration.
c. Bidder should develop an appropriate policy, processes and procedures for failover and fall back to DR site in case of a disaster. An Active-Active configuration is proposed. However, Bidder should perform a risk assessment and the business impact analysis for DDA. Bidder should develop emergency response and operations plan and present it to DDA management.
d. Bidder should design architecture for implementation of the replication of data from the DC to the DR site. It is expected that Bidder will draw knowledge from industry best practices and its experiences to implement the replication solution and BCP policy that is best suited for DDA. Bidder shall document the blueprint for BCP policy and cohesive replication architecture and obtain approval from the DDA prior to actual implementation.
e. Bidder would be required to establish the data archival policies along with the procedures with the DDA.
f. Bidder shall ensure in there recommended design data backup till the last transaction occurring in the system to ensure enhanced service levels and following RPO and RTO objectives:
   i RPO<=30 minutes and RTO <=3 Hrs
g. Any storage space / media required to maintain backups and other requirements of the RFP should be provisioned for by the selected Bidder in his Bid.
h. Designing and implementing data synchronization procedures for the DR Site. Periodic testing may be done to ensure that all replication and data synchronization procedures are in place all the time. Replication between Data Centre and DR Site as well as change-over during disaster should be automatic and real-time for minimal impact on user experience.

1.2.2 Operation and Maintenance Phase

The selected Bidder is responsible for the day to day maintenance of the system for the entire period of Contract. For the IT Infrastructure procured as part of this RFP, the selected Bidder will be responsible for smooth Operations and Maintenance for the entire duration of the contract and shall provide

a. Onsite Warranty support
b. Annual Technical Support (ATS) for all the licensed software
c. Providing Help desk support with Escalation matrix for registration of complaints related to software procured through this by DDA
d. Change Management including maintenance of development environment for the entire project duration
e. Provide and maintain SMS, Email and online payment services.

1.2.2.1 Overview of Post Implementation Services

An indicative list of activities and nature of support to be provided is mentioned below:

a. System Administration and Trouble Shooting
    i Overall monitoring of all IT and Non-IT infrastructure deployed at DDA for the Project including Network &Server Infrastructure at DC/DR & Departmental locations, networking equipment& connectivity, system software, application, database, and all other services associated with these facilities to ensure service levels, performance and availability requirements as prescribed in the RFP as per well-defined Standard Operating Procedures prepared by bidder and approved by DDA.
    ii Scheduled and ad hoc maintenance (on need basis) and operations like Data backup, replication, patch management and upgrades
    iii Perform system administration tasks such as managing the user access, creating and managing users, taking backups etc.
    iv Performance tuning of the system to ensure adherence to SLAs and performance requirements as indicated in the RFP.
    v Proper configuration of server parameters, operating systems administration and tuning. Bidder would be a single point of accountability for all hardware maintenance and support central infrastructure.
    vi Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of upgrades including migration to higher versions and patches to ensure that the system is properly updated. Bidder is also responsible for re-installation in the event of system crash/failures.
    vii Regular monitoring and maintenance a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc. Bidder should also ensure that the bottlenecks in the infrastructure are identified and fine tuning is done for optimal performance.
    viii Regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. Bidder should undertake actions in accordance with the results of the log analysis. The system administrators should also ensure that the logs are backed up and truncated at regular intervals.

ix Adopt a defined process for change and configuration management in the areas including, but not limited to, changes in parameter settings for application, servers, operating system, devices, etc., applying patches, etc.

x Bidder to establish and implement leading practices of IT service Management like Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO)/IEC 20000 standard and ISO 27001 which shall promote the adoption of an integrated process approach to effectively deliver managed services and address security concerns to meet the requirements of DDA;

xi The Bidder should identify all assets and document the importance of these assets. The asset inventory should include all the information necessary in order to recover from a disaster, including type of assets, format, location, backup information, license information etc.

xii Bidder to establish basic tools for Data Centre (DC) IT management to undertake health check monitoring, troubleshooting etc. with semi-automation of DC operations.

b. Database, Backup Administration and Trouble Shooting

Undertake end-to-end management of database on an on-going basis to facilitate smooth functioning and optimum utilization including regular database backup and periodical testing of backup data, conducting configuration review to tune database, maintaining the necessary documentation and managing schemes to database schema, disk space, user roles, and storage. Indicative list of activities to be performed by the bidders is:

i Perform Backup of storage as per the defined policies by DDA and Bidder

ii Monitoring and enhancing the performance of scheduled backups, Schedule regular testing of backups and ensuring adherence to related retention policies as defined by DDA

iii Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.

iv Real-time monitoring, log maintenance and reporting of backup status on a regular basis.

v Conduct code and configuration reviews to provide inputs to DDA in order to improve the performance or resolve bottlenecks if any.

vi Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.

vii Report backup status on a regular basis and ensure prompt problem resolution in case of failures in the backup processes.

viii Manage database upgrade or patch upgrade as and when required with minimal downtime.

ix Regular backups for all databases in accordance with the backup and archive policies and recovery whenever required with appropriate permissions. Testing of backup media should be undertaken from time to time to ensure availability of data. Bidder should co-ordinate with DDA management for back-up activities. Indicative data-backup & storage requirements:

c. Security Administration, Maintenance and Management Services

The Bidder should ensure adherence to the following pre-requisites

i Management of security environment of the central IT application to maintain performance at optimum levels.

ii Bidder will perform security incident management and internal audit

iii Respond to security breaches or other security incidents and coordinate with stakeholders in case of a new threat is observed to ensure that workaround / patch is made available for the same.

iv Perform reactive and preventive maintenance exercise

d. MIS Reports and Incident Reporting

The following is an indicative list of MIS reports to be submitted by the bidder post go-live. The selected Bidder shall also draw an exhaustive list of reports along with DDA. Bidder shall submit the reports on a regular basis in a mutually decided format. Bidder shall submit 1 hard copy and 1 soft copy of each of the reports. Indicative list if provided below:

i System generated log of all the calls / emails should be maintained at helpdesk and facility management team and through the ticketing system. This log should also work as SLA monitoring mechanism for all the SLAs of helpdesk as mentioned in Section 3 of this RFP

ii Network Availability and Utilization Report.

iii Asset modification report at the DDA office locations sites and datacentre locations.

iv Summary of component wise uptime in the datacentre.

v Summary of resource utilization of all components in the datacentre.

vi Log of preventive / break-fix maintenance undertaken.

vii Summary of changes undertaken in all the datacentres including major changes like configuration changes, release of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

viii Consolidated SLA / non-conformance report

ix Asset database report and Asset Audit report

x Summary of incidents reported like Application down, Components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization, etc.

xi Feedback report from users for the services rendered.

xii Bug / defect resolution reports including the analysis of bugs / defects resolved, pending, completion time, responsiveness, concern areas, etc.

xiii Change Request Logs with their resolution status

xiv Incident Reporting (as and when it occurs)

xv Complete system down – with root cause analysis

xvi Peaking of resource utilization on any component

xvii Bottlenecks observed in the system and the possible solutions and workarounds.

xviii Security Incident Reporting (as and when it occurs)

xix Detection of security vulnerability detection with the available solutions / workarounds for fixing.

xx Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.

.

e. Facility management Services
   i The Bidder shall provide Facilities Management Services (helpdesk services and software technical support services) to DDA.
   ii The bidder is required to deploy minimum resources as mentioned in Annexure 33.

f. Overall
   i Ensure to undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any incidents) and coordinate with OEM/Hardware vendor for necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours of DDA unless inevitable and approved by the *DDA*
   ii Ensure to undertakes reactive maintenance (any corrective action, maintenance activity that is required post the occurrence of an incident) that is intended to troubleshoot the system with sufficient teams
   iii A control room would be set up at DDA Head Quarters where monitoring of entire application, MPLS/internet link and hardware would take place using Dashboards. Control room would have representative from Bidder and appointed officials from DDA
   iv Escalate and co-ordinate with its OEMs for problem resolution wherever required
   v The selected Bidder will be required to comply with various policies relating to monitoring and management of infrastructure such as IS Policy, backup and archival policy, system software update policy etc. of DDA

1.2.2.2 Annual Technical Support (ATS)

As part of the ATS services System Integrator shall provide:

1. System Integrator shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.
2. If the additional copies of Operating System are required to be installed/ reinstalled / de-installed, the same should be done as part of ATS.
3. System Integrator should carry out any requisite adjustments / changes in the configuration for implementing different versions of Application Software.
4. Updates/Upgrades/New releases/New versions/Patches/Bug fixes: The System Integrator shall provide from time to time the Updates/Upgrades/New releases/New versions/Patches/Bug fixes of the software, operating systems, etc. as required. The System Integrator should provide free Updates/Upgrades/New releases/New versions/Patches/Bug fixes of the software and tools to DDA as and when released by OEM.
5. Software License Management. The System Integrator shall provide software license management and control. System Integrator shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance.
6. System Integrator shall have complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. System Integrator shall provide a single-point-of-contact for software

support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.

1.2.2.3 Help Desk and Trouble ticket management system

1. The selected Bidder as part of provisioning support for Department users at each location and the DC will setup centralized helpdesk and coordinate with the respective OEMs of the IT Infrastructure deployed at DC and the Department offices. The selected Bidder will undertake the following:
    a. Provide Help Desk services to track and route requests for service and to assist department users in answering questions and resolving problems related to the IT Infrastructure installed at Data Centre and at all the Department Offices .
    b. Become the central collection point for contact and control of the problem, change, and service management processes (This includes both incident management and service request management)
    c. Shall provide a first level of support for application and technical support at CMS implementation locations across DDA where the software, hardware, and other infrastructure will be rolled out.
    d. Provide the following integrated customer support by establishing <9 hrs X 6 days> Help Desk facility for reporting issues/ problems with the software, hardware and other infrastructure.
2. This shall be an online system deployed centrally and shall be used by the selected Bidder extensively for management of network support activity and handling calls from citizen, departmental staff, any other stakeholders. Service desk is an application that facilitates the end-to-end service support. The proposed system should include required hardware and software.
3. During and after the end of the project period, the System Integrator shall refrain from canvassing DDA and any of its associates with any claim for employment of bidder's personnel deployed under the project.
4. The System Integratorwill deploy helpdesk management system (web enabled with SMS/WhatsApp and e-Mail based alert system) for Helpdesk Call management and SLA reporting..
    a. User Interface: - The proposed system should have an easy to use user interface (preferably a browser based), so that users across DDA can lodge any complaints and service requests. The solution shall have a reporting interface with a consolidated view of the network status. All users (departmental and external) of the system should be able to log a request in the system using any of the following channels:
        i Telephonic call on the Toll-free Helpline (DDA will provide the telephone)
        ii email
        iii Online chat on the departmental web-portal
        iv Through intranet for departmental users or web-portal for external users
    b. Complete incident and problem management: - Service desk should address both Incident Management and Problem Management. The application should maintain a classification system that will distinguish the single occurrence trouble tickets or incidents needing immediate resolution from in-depth root cause analyses that may require longer term to resolve a problem.
    c. The flow of events at the call centre should be:
        i Event is triggered and forwarded to service desk.

ii Service desk submits and updates the trouble ticket.

5. Tasks expected:
   a. Ticket mapping and allocation: According to the severity, the ticket should be given the priority level. Also it should map the ticket to the appropriate personnel for the resolution.
   b. Updating the status: Update the status of ticket.
   c. It should be able to log and escalate user interactions and requests.
   d. It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
   e. Status of registered calls with interface for Call centre, using which call centre can inform the status to users over phone.
   f. Historical report indicating number of calls, time to resolve, status etc. for a specified period of time.

1.2.2.4 Other Requirements

1. All relevant infrastructure and supporting system software required for the deployment and operation of the help desk is to be provided by the selected Bidder.
2. The system deployed by the System Integrator shall be complied with ITIL and ISO 20000 service specifications. Any additional licence required for the IT helpdesk shall be asserted by the System Integrator
3. Bidder should arrange for desktops / workstations, printers and other peripherals and consumables for its team members deployed.DDA shall provide furniture, space, phone lines and Internet.
4. For helpdesk support, the PCs will be provided by hardware vendor on behalf of DDA. The bidder for this RFP will only be required to provide manpower for helpdesk and the required application for helpdesk support.
5. Bidder should have to arrange for necessary tools for defect tracking, defect logging, application performance monitoring, automatic testing etc. to deliver the complete software development and maintenance services.
6. Bidder should ensure the usage of configuration management and version control tool and own the necessary licenses for its team to deliver software development and maintenance services. Additionally, Bidder should provide license for the configuration management and version control tool for the Purchaser.
7. Bidder should predominantly carry out all the software development of DDA's major core modules and its integration at DDA premise. For other general modules, offshore software development can be considered by DDA on special request of bidder.
8. The Bidder will be responsible for providing the necessary development and testing environment and maintaining the related software and hardware for the Contract period.
9. All the assets should be handed over to the Department at the end of the Contract period.
10. During the Contract period, all project assets including data and intellectual property should be in safe custody and due reasonable care should be taken on the behalf of the Department to prevent any unauthorized use.

1.2.3 Licensing Requirements

1. All system software, production licenses, such as Operating system, database middleware, EMS& Helpdesk, etc. have to be procured in the name of the DDA
2. The licenses should be perpetual and enterprise wide for the core application and other software unless otherwise stated. The software licenses shall not be restricted based on

location and the *DDA* should have the flexibility to use the software licenses for other requirements, if required

1.2.4 Asset Management

The selected Bidder will perform the following asset management functions with respect to the infrastructure deployed at various locations:

a. Take periodic stock of, review physical inventory and maintain stock registers of hardware at all locations covered under this Project. The selected Bidder would maintain stock registers as per format agreed with the *DDA*
b. Maintain documentation of the hardware assets, maintain asset Information for all Project locations, on parameters to be mutually agreed between the *DDA* and the selected Bidder, which shall include details like -
    i Product type, model number, version number
    ii Manufacturer
    iii Office location
    iv Maintenance status, etc.
c. Update or correct the asset information following any new installations, movement, addition, or change performed by the selected Bidder.
d. Produce periodic reports and machine readable files in agreed upon format pertaining to some or all of the asset information.
e. Restrict movement of server/equipment/items in or out of DC/DR or any other location under the Project without prior permission from the *DDA*

1.2.5 Knowledge Transfer

1. At the end of the Contract period, the selected Bidder will be required to provide necessary handholding and transition support to designated staff or any other agency that is selected for maintaining the system post the Contract with the selected Bidder. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.
2. Knowledge Transfer is an integral part of the scope of work of the selected Bidder. This will have to be done even in case the Contract with the Bidder ends or is terminated before the planned timelines.

Please note that this is only an indicative list. Any other activity, over and above these, as may be deemed necessary by the selected Bidder to meet the service levels and requirements specified in this Contract are also required to be performed by the selected Bidder at no additional cost.

1.2.6 Exit Management

1.2.6.1 Purpose

In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

1.2.6.2 Transfer of Assets

1. *DDA* shall be entitled to serve notice in writing on the System Integrator at any time during the exit management period as detailed hereinabove requiring the System Integrator and/or its sub-contractors to provide the *DDA* with a complete and up to date list of the Assets within 30 days of such notice. *DDA* shall then be entitled to serve notice in writing on the System Integrator at any time prior to the date that is 30 days prior to the end of the exit management period requiring the System Integrator to sell the Assets, if any, to be transferred to *DDA* or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.
2. In case of contract being terminated by *DDA*, *DDA* reserves the right to ask System Integrator to continue running the project operations for a period of 6 months after termination orders are issued.
3. Upon service of a notice under this Article the following provisions shall apply:
    a. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the System Integrator, the System Integrator shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the DDA
    b. All risk in and title to the Assets to be transferred / to be purchased by the *DDA* pursuant to this Article shall be transferred to *DDA* on the last day of the exit management period.
    c. *DDA* shall pay to the System Integrator on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule.
    d. Payment to the outgoing System Integrator shall be made to the tune of last set of completed services / deliverables, subject to SLA requirements.
    e. The outgoing System Integrator will pass on to *DDA* and/or to the Replacement System Integrator, the subsisting rights in any leased properties/ licensed products on terms not less favourable to *DDA*/ Replacement System Integrator, than that enjoyed by the outgoing System Integrator.

1.2.6.3 Cooperation and Provision of Information

During the exit management period:

a. The System Integrator will allow the *DDA* or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the *DDA* to assess the existing services being delivered;
b. promptly on reasonable request by the *DDA* the System Integrator shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the System Integrator or sub-contractors appointed by the System Integrator). The *DDA* shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The System Integrator shall permit the *DDA* or its nominated agencies to have reasonable access to its employees and facilities as reasonably required by the Chairman, PIU to understand the methods of delivery of the services employed by the System Integrator and to assist appropriate knowledge transfer.

1.2.6.4 Confidential Information, Security and Data

1. The System Integrator will promptly on the commencement of the exit management period supply to the *DDA* or its nominated agency the following:
   a. information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
   b. documentation relating to Computerization Project's Intellectual Property Rights;
   c. documentation relating to sub-contractors;
   d. all current and updated data as is reasonably required for purposes of *DDA* or its nominated agencies transitioning the services to its Replacement *System Integrator* in a readily available format nominated by the *DDA* its nominated agency;
   e. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable *DDA* or its nominated agencies, or its Replacement <<*'System integrator'*>> to carry out due diligence in order to transition the provision of the Services to *DDA* or its nominated agencies, or its Replacement *System Integrator* (as the case may be).
2. Before the expiry of the exit management period, the System Integrator shall deliver to the *DDA* or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the System Integrator shall be permitted to retain one copy of such materials for archival purposes only.
3. Before the expiry of the exit management period, unless otherwise provided under the MSA, the *DDA* or its nominated agency shall deliver to the System Integrator all forms of System Integrator confidential information, which is in the possession or control of Chairperson, PIU or its users.

1.2.6.5 Employees

1. Promptly on reasonable request at any time during the exit management period, the System Integrator shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the *DDA* or its nominated agency a list of all employees (with job titles) of the System Integrator dedicated to providing the services at the commencement of the exit management period.
2. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the System Integrator to the *DDA* or its nominated agency, or a Replacement System Integrator ("Transfer Regulation") applies to any or all of the employees of the System Integrator, then the Parties shall comply with their respective obligations under such Transfer Regulations.
3. To the extent that any Transfer Regulation does not apply to any employee of the System Integrator, department, or its Replacement System Integrator may make an offer of employment or contract for services to such employee of the System Integrator and the System Integrator shall not enforce or impose any contractual provision that would prevent any such employee from being hired by DDA or any Replacement System Integrator.

1.2.6.6 Transfer of Certain Agreements

On request by the *DDA* or its nominated agency the *System Integrator* shall effect such assignments, transfers, licences and sub-licences as DDA may require in favour of the DDA or its Replacement *'System integrator'* in relation to any equipment lease, maintenance or service provision agreement between *'System integrator'* and third party lessors, vendors,

and which are related to the services and reasonably necessary for the carrying out of replacement services by the *DDA* or its nominated agency or its Replacement *'System integrator'*.

1.2.6.7 Rights of Access to Premises

1. At any time during the exit management period, where Assets are located at the *System Integrator*'s premises, the *System Integrator* will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) the *DDA* or its nominated agency and/or any Replacement *System Integrator* in order to make an inventory of the Assets.
2. The *System Integrator* shall also give the *DDA* or its nominated agency or its nominated agencies, or any Replacement *System Integrator* right of reasonable access to the Implementation Partner's premises and shall procure the *DDA* or its nominated agency or its nominated agencies and any Replacement *System Integrator* rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the MSA as is reasonably necessary to migrate the services to the *DDA* or its nominated agency, or a Replacement *System Integrator*

1.2.6.8 General Obligations of the System Integrator

1. The *System Integrator* shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the *DDA* or its nominated agency or its Replacement *System Integrator* and which the *System Integrator* has in its possession or control at any time during the exit management period.
2. For the purposes of this Schedule, anything in the possession or control of any *System Integrator*, associated entity, or sub-contractor is deemed to be in the possession or control of the *System Integrator.*
3. The *System Integrator* shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

1.2.6.9 Exit Management Plan

1. The *System Integrator* shall provide the *DDA* or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.
    a. A detailed program of the transfer process that could be used in conjunction with a Replacement *System Integrator* including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
    b. plans for the communication with such of the *System Integrator*'s sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the *DDA*'s operations as a result of undertaking the transfer;
    c. (if applicable) proposed arrangements for the segregation of the *System Integrator*'s networks from the networks employed by *DDA* and identification of specific security tasks necessary at termination;
    d. Plans for provision of contingent support to *DDA* and Replacement *System Integrator* for a reasonable period after transfer.

2. The System Integrator shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
3. Each Exit Management Plan shall be presented by the System Integrator to and approved by the *DDA* or its nominated agencies.
4. The terms of payment as stated in the Terms of Payment Schedule include the costs of the System Integrator complying with its obligations under this Schedule.
5. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.
6. During the exit management period, the System Integrator shall use its best efforts to deliver the services.
7. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
8. This Exit Management plan shall be furnished in writing to the *DDA* or its nominated agencies within 90 days from the Effective Date of the Agreement.

1.3 Design, Deployment and operations and maintenance of IT Infrastructures of CMS at Data Centre and Data Recovery Centre Service Provider

1.3.1 Broad Scope

The service provider has to provide sufficient space to co-host the DDA's DC IT Infrastructure and DR infrastructure. The Data centre should be at least Tier 3 Data Centre. The bidder should also provide Sufficient uninterrupted power, electrical connections, air conditioning, backup power through UPS and Generator, telecom facilities (As part of telecom facility SP shall provide necessary junction box / space in the telecom room for multiplexer/s and other equipment's, Surveillance, access control system, fire suppression system, physical security and soft services as applicable for Data Centre and Disaster Recovery as required for the proposed equipment on 24 x 7 basis, in order to maintain uptime of all such facilities as per SLA. The complete electrical work is to be performed by the bidder by working back with the DDA and its designated Service provider. Hosting Provider shall also be responsible for extending all links from its communication room to the server cage area allocated to the DDA.

The site offered for co-hosting the DC should confirm to the minimum specifications as set out in the detailed requirement in sub sequent sections of this RFP. The bidder shall maintain & manage all the facility provided by the SP to host DDA's DC and DR IT Infrastructure.

The proposed DC should be Tier 3 Data Centre. The bidder shall provide sufficient electrical connections, HVAC, backup power through UPS and Generator, network communication facilities, Surveillance, access control system, fire suppression system, physical security and soft services etc. as applicable for DC and as required for the proposed equipment on 24 x 7 basis in order to maintain uptime of all such facilities at as per SLA.

1.3.2 General Requirements

a. The proposed Data Centre should be at least Tier 3 compliant.

b. The proposed DC site should comply with the technical requirements specified in Annexure 2 of this RFP Annexures.
c. The power should be available from two different power sources. Two separate power paths from the UPS to be provided to the Server room area and the network communication area.
d. The UPS should be configured in redundant (1 + 1) mode.
e. Entry and exit at the Data Centre premise (Building), Server room / Hall area, server cage area, and network communication room should be restricted and monitored. Security for the building should be made available 24*7 at the entry / exit levels and having adequate access control mechanism in place.
f. The doors for the server room, communications room, and other critical
g. Areas beyond level 2 should be fire rated.
h. The entire facility should be automatic with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source.
i. 99.98% uptime is required for the DC Environmental Infrastructure and services.
j. The Data Centre facility building should be designed and constructed for Earthquake resistance and should be away from hazardous chemical materials.

1.3.3 Server Room Area

a. The Server room proposed by the bidder should be at least tier 3 compliant.
b. DDA envisages requirement of a dedicated clear space of 1500 sq. feet to host DDA's DC IT infrastructure in the server room area. The exact number of rack & space, power requirement and other information shall be separately given to the successful bidder. However, Service provider is expected to quote per rack space, charges. DDA envisages an addition of couple of more racks in the Server cage area. However, should there be requirement of additional space in the future, other than the space for existing racks & additional 2 racks, the bidder should be able to provide the same on the prorated per square feet cost within the same facility on the same floor of the proposed server cage area.
c. The bidder shall provide a dedicated server cage area for the DDA in the server room/ Hall area. The cage area should secure the allocated space to the DDA.
d. The server cage entrance & exit should be accessible using the proximity card (access control system).
e. The entry to server room / Server Hall area should be accessible using Biometric access.
f. The Server room / Server Hall should have precision air conditioning with redundancy.
g. The bidder shall provide adequate power points in the Server cage area allocated to the DDA. The bidder shall quote as per the financial bid template provided in Annexure of this RFP. **The DDA will pay only for consumed power**. The DDA requires a power meter that can measure the exact power consumed by the DDA's equipment in the DDA's server caged area. This consumed power will be payable by the DDA at the unit rates provided in the commercials throughout the tenure of the contract.
h. The bidder shall provide power connectors / sockets.
i. Single phase and three phase power should be made available to support DDA's equipments in the caged area.

Note: The information provided above is an estimated requirement and the DDA reserves the right to change the quantities/requirements. The exact requirements will be provided to the successful bidder and the unit rates provided for these requirements would be considered for those changed requirements.

j. The service provider will be responsible for extension of links from SP telecommunication room to server cage area irrespective of whether the communication links are taken from the SP. The bidder shall extend such links from their network communication room to the server cage area provided to the DDA to host their DC infrastructure. Such cost should be included in the onetime expense in the commercial.

k. Bidder in their technical bid shall provide the proposed Server caged area layout clearly showing the placement of the racks in the server caged area along with indicative positioning of the BMS equipment like CCTV cameras, Fire/ smoke detectors, access control system, rodent repellent etc.

1.3.4 Communication Area

a. The bidder in their communication area shall have Telecom junction box /multiplexers of various link service providers and should be available in and around the facility building for DDA's use.

b. The Data Centre Service provider should allow the termination of the links provided by the DDA appointed link service providers. If Telecom junction box / multiplexers of these link service providers are not available, then the DC service provider should allow the commissioning of the same. The DC SP shall also allow laying of cables and associated works in their premises.

c. The link extension from the DC service provider's communication room till the server cage area will be done by the DC service provider.

1.3.5 BMS (Building Management Systems)

a. The SP shall provide Access cards, Gate passes to the DDA's personnel, DDA appointed representatives, bandwidth service provider and any other DDA approved authority as and when they would visit the site. SP should agree that such access can be provided 24 X 7 and will not have any time restriction.

b. The SP shall regularly monitor the access to the DDA's Server room / cage by means of access control system, physical security, Biometric access and CCTV and should always make sure that they are functional 24X7 days.

c. If required by the DDA the SP should be able to provide details of people accessing the DDA's Server room / cage by sharing the entries made in the security register, reports from access control system, CCTV video clips etc.

d. The SP shall make sure that the required power, air conditioning, security system and other facilities provided to the DDA is always available (24X7 days).

e. The SP shall provide Fire detection & suppression system exclusively for the server room caged area. Fire detection and suppression can be common however the areas allocated to the DDA should be well within the coverage of fire detection and suppression.

f. The Server room area should be provided with Water Leak detection system and fire alarm system. The facility areas proposed for the DDA should be well within the coverage of water leak detection system

g. There should be CCTV monitoring for surveillance of building entrance, exits and other critical areas where DDA's components are placed. Activities to be recorded and the archival should be kept for at-least one month.

h. The data centre should have electronic rodent control systems with operating ability on varied frequency range. The facility areas – Server room area / server caged area, communication room should be well within the coverage of the rodent repellent.

i. All the Building Management system (BMS) activities are to be controlled centrally in a room specifically to be used for BMS activities. The vendor should manage the BMS activities on a 24*7 basis or as the DDA decides.

1.3.6 Miscellaneous

a. The SP shall provide contacts and escalation matrix to log the complaints / problems faced in the facility provided to the DDA.

b. SP shall provide all necessary help to the DDA appointed Service provider or Vendor while moving the DDA equipment into the site. For example entry permission for vehicles carrying equipments, parking of such vehicles to be closer to the lift till the time the equipment are being offloaded, use of lift / service lift, assist in procedures documentation, providing trolley to carry heavy equipments to the allocated cage / room, etc. The DDA should not incur any extra cost for availing these said services.

c. The DDA may in future require additional space at the Data Centre site. The SP agrees that in the event the DDA wants additional space for expansion; the same will be provided to the DDA within the same DC site / floor or building. The rate per square feet would be mutually agreed at the time of such expansion. However, the vendor agrees that the rate for expansion shall not exceed the current rates agreed. DDA cannot provide any time frame to inform SP for taking up additional space.

1.3.7 Communication Links

a. SP provider has to procure, manage infrastructure and services for the Network and Bandwidth to connect all DDA offices with Data Centre, DC and DR connectivity. The hosting service provider has to assure that the termination of these links is feasible at the proposed site

b. The SP shall make sure that the multiplexers / Junction boxes these link service providers are available at the proposed site

c. The SP shall extend the connection from the Multiplexers / Junction boxes to the DDA's server caged area.

d. The DDA may or may not procure the links from the SP. However, in case DDA felt the need to have links from hosting service provider (the successful bidder of this RFP). The same shall be provided as per detailed in RFP Vol III.

e. The SP shall provide the links between DDA's hosting Data Centre and DDA's DR site so as to meet theSLA's mentioned in volume III of this RFP.

f. The service provider shall also quote for the bandwidth and other charges for connecting DDA offices with the Data Centre as detailed out in RFP Vol III.

g. The SP shall provide the link monitoring facility to the DDA which will enable the DDA to monitor the links in real-time from their Data Centre. DDA should be able to monitor following parameters:

   i Link Latency

ii Bandwidth utilization

iii Packet loss

h. The above parameters are minimum requirement. The monitoring facility shall provide other link related monitoring parameters that may be required to monitor the SLA.

i. Any equipment / software requirement in order to achieve the above mentioned facility, the SP should factor such cost in one-time link implementation cost. SP should manage and maintain this equipment throughout the contract tenure.

j. SP should provide the link performance report to the DDA on monthly basis. The SP shall provide the on-demand links between Near Site & DR during DR Failover or DR drill. Minimum will be 2 Mbps and Maximum will be 100Mbps. The SP should be able to provide the desired bandwidth within 60 minutes from such request made by the DDA by email / letter / phone call by DDA authorized personnel.

1.3.8 Seating Space

DDA is in process of setting up of a Network Operation Centre (NOC) at its Vikas Sadan, New Delhi office. The number of resources required, the infrastructure, and connectivity has already been taken care by DDA.

a. The DDA will require separate enclosed dedicated seating space at the DC in the seating area. DDA anticipates the seating space for 2 DDA appointed personnel. SP shall factor for at least 30 Square feet work area per seat. In addition, SP shall provide adequate space for the movement within the enclosed seating area. SP is required to provide the cost for this seating space as per the format provide in the RFP. The cost should be provided for per seat per annum.

b. The UPS / generator backup power facility needs to be available to the proposed seating area. SP shall provide UPS backed up 3 power points per seat.

c. The seating area should be provided with comfort air conditioning.

d. The SP shall provide Tables, chairs, drawers with locking facility, telephone extensions for communication between Server cage area and the seating area, in the seating area for 10 personnel. The furniture to be provided by the SP here, refers to modular furniture with sufficient seating, personal storage and workspace for each individual person.

e. The seating area furniture should be modular furniture with drawers/pedestal, keyboard tray, for each table. Lockers that can accommodate 3 box files and some stationary, the one that comes with the work table. This will be for every seat.

f. The SP shall provide access control system for controlling access to the seating area which will be centrally monitored by SP through their BMS system. The SP shall provide the cards to the DDA's authorized onsite resources. This access control system should be managed & monitored by the SP through their BMS system.

g. The SP shall provide the network connectivity from the seating space provided by the SP to the DDA's server caged area. For each seat the SP shall provide redundant network points (2 points).

h. All such costs should be included as the cost for "seating space". The two number of seats provided by the DDA is for the TCO purpose, however DDA may alter the quantity of number of persons depending on the DDA's need and the payment will be made on the prorated calculation.

i. The seating area should include the desk, chair, one cabinet per seat, power connections and network connections (two per seat)

j. SP shall provide the proposed seating area layout clearly indicating the total space being factored for the dedicated seating area in their technical bid submission

1.3.9 Service Levels

The facilities like power, cooling, CCTV monitoring, security (biometric, physical, access card) provided by the service provider to co-host DDA's DC equipment's should have high availability. The Service Levels for Links provided and monitored by SP will be as per Volume III of this RFP document.

1.3.10 Data Center Operations & Business Continuity Planning

The selected Bidder in consultation with DDA Service provider or its authorized agency is expected to support DDA's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for DDA carried out by the Hardware & Application Vendor. An indicative list of activities to be performed by the selected Bidder is mentioned below:

a. Designing and implementing business continuity and restoration procedures for the IMS application
b. Ensuring that there is no single point of failure and adequate level of redundancy is built in to meet the uptime and other requirements of this RFP.
c. Bidder should develop an appropriate policy, processes and procedures for failover and fall back to DR site in case of a disaster. An Active-Active configuration is proposed. However, Bidder should perform a risk assessment and the business impact analysis for DDA. Bidder should develop emergency response and operations plan and present it to DDA management.
d. Bidder shall facilitate data archival along with DDA.
e. Bidder shall ensure data backup till the last transaction occurring in the system to ensure enhanced service levels and following RPO and RTO objectives:
    i RPO<=30 minutes and RTO <=3 Hrs
f. Supporting data synchronization procedures for the DR Site. Periodic testing may be done by DDA/Authorised agency to ensure that all replication and data synchronization procedures are in place all the time. Replication between Data Centre and DR Site as well as change-over during disaster should be automatic and real-time for minimal impact on user experience.
g. MIS Reports and Incident Reporting-The following is an indicative list of MIS reports to be submitted by the bidder post go-live. The selected Bidder shall also draw an exhaustive list of reports along with DDA. Bidder shall submit the reports on a regular basis in a mutually decided format. Bidder shall submit 1hard copy and 1 soft copy of each of the reports. Indicative list if provided below:
    i System generated log of all the calls / emails should be maintained at helpdesk and facility management team and through the ticketing system. This log should also work as SLA monitoring mechanism for all the SLAs of helpdesk as mentioned in Section 3 of this RFP
    ii Asset modification report at the DDA office locations sites and datacentre locations.

iii Summary of resource utilization of Power & cooling components in the datacentre.

iv Log of preventive / break-fix maintenance undertaken.

v Summary of changes undertaken in all the datacentres including major changes like configuration changes.

vi Consolidated SLA / non-conformance report

vii Summary of incidents reported like Application down, Components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization, etc.

viii Feedback report from users for the services rendered.

ix Change Request Logs with their resolution status

x Incident Reporting (as and when it occurs)

xi Complete system down – with root cause analysis Peaking of resource utilization on any component

xii Bottlenecks observed in the system and the possible solutions and workarounds.

xiii Security Incident Reporting (as and when it occurs)

1.3.11 Other Requirements

a. All relevant infrastructure and supporting system software required for the deployment and operation of the help desk is to be provided by the selected Bidder.

b. Bidder should arrange for desktops / workstations, printers and other peripherals and consumables for its team members deployed.

c. Bidder should have to arrange for necessary tools for defect tracking, defect logging, application performance monitoring, automatic testing etc. to deliver the complete software development and maintenance services.

d. During the Contract period, all project assets including data and intellectual property should be in safe custody and due reasonable care should be taken on the behalf of the Department to prevent any unauthorized use.

1.3.12 Knowledge Transfer

a. At the end of the Contract period, the selected Bidder will be required to provide necessary handholding and transition support to designated staff or any other agency that is selected for maintaining the system post the Contract with the selected Bidder. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.

b. Knowledge Transfer is an integral part of the scope of work of the selected Bidder. This will have to be done even in case the Contract with the Bidder ends or is terminated before the planned timelines.

Please note that this is only an indicative list. **Any other activity, over and above these, as may be deemed necessary by the selected Bidder to meet the service levels and requirements specified in this Contract are also required to be performed by the selected Bidder at no additional cost.**

1.4 Supply, Deployment And Maintenance Of Hardware

The broad scope of includes

a. Procurement, deployment and maintenance of required IT Equipment's at Data Centre& DR Site;
b. Procurement, deployment, operationalization and maintenance of IT Infrastructure at all office locations of DDA;
c. Other activities as listed in this RFP.

The hardware as specified in Annexure 32 shall be provided by vendor, selected through this procurement process. The following services shall also be provided by the selected bidder :

a. Deployment and commissioning of required hardware as per the plan to be provided by DDA
b. Submit Installation and Commissioning reports
c. Provide onsite warranty services and equipment maintenance
d. Provide AMC support for the entire duration so as to maintain the service levels specified in Annexure III.
e. Bidder shall coordinate with DDA to resolve any problems encountered during and after rollout. All post commissioning issues shall be documented and the necessary resolutions shall be done by bidder.

1.4.1 Supply / Procurement of IT Infrastructure at DC DR site, and DDA offices.

a. Bidder needs to provide Hardware as listed in Annexure 32 exclusively for this project.
b. Bids / proposals which do not meet the minimum IT infrastructure specifications given in this RFP will be summarily rejected.
c. The IT Infrastructure proposed should be purchased **within last 1 months** from the date of deployment and documentary proof for warranty and proof of purchase should be produced at the time of deployment of infrastructure.
d. The Bidder should provide requisite licenses for all the system software required for servers including, but not limited to industry standard operating system, OS hardening.
e. The Bidder will be responsible for providing all the details of the Bill of Material (BoM) and specifications of the IT Infrastructure proposed, all other equipment proposed as part of its Technical Proposal. The financial quote submitted by the Bidder should include costs for these.
f. The bidder shall ensure that all invoice of OEM are in the name of DDA. Bidder shall mandatorily submit all invoice to DDA.
g. The technical documentation involving detailed instruction for operation and maintenance is to be delivered with every unit of the equipment supplied. The language of the documentation shall be in English. Such manuals shall include illustrated catalogues, reference manuals, technical manuals and operation manuals for the purpose of operating the solution. Complete documentation should include:

i Hardware Manuals

ii Operating System(s) Manuals

h. The sets of documents and manuals, supplied and delivered by the proponent shall be in reasonable detail and be current at the time of delivery; be in English language; include system operations, operating system and the Third Party software products if any; include error failure recovery instructions; include hardware and software debuggers/diagnostics/listing; include ready reference; and include illustrated parts and catalogues.

1.4.2 Installation and Commissioning of IT Infrastructure

1. The selected Bidder is responsible for installation and configuration of the entire infrastructure set-up, including but not limited to the following:
   a. All IT Infrastructure including operating systems and any other system software required for making the infrastructure operational and tuned for satisfactory performance.
   b. The IT Infrastructure will be installed and configured in accordance with the IT Policies of DDA
   c. The selected Bidder will ensure that the reports for monitoring of SLAs such as system uptime, performance, etc. are generated automatically from the system and the applicable penalties are calculated as indicated in the RFP.

1.4.3 Manpower Requirements

1. The project would require minimum provisioning of dedicated manpower at DDA Offices as detailed in Annexure 33. The Bidder shall estimate the resourcing requirement and may quote for resource requirement above the minimum requirement.
2. The bidder would be required to position resources to provide hardware related technical support at each of the offices during the roll out period and post go live period.
3. The Technical support resources would be required to work closely with the Project Manager and PMU in ensuring adherence to the project timelines.
4. The bidder should ensure that the roster schedule of all deployed manpower for each day at the required locations has been communicated in advance to DDA. No change to the deployed staff shall be done by the bidder without written approval from the DDA.
5. Adherence to all laws pertaining to personnel, labour laws, etc. for any manpower deployed by the bidder on this Project shall be the responsibility of the bidder
6. The bidder would issue Identity cards to each of the staff members deployed at the sites
7. The bidder will maintain adequate leave reserve for the staff, so that the work in the respective offices remains unaffected in all cases.

1.4.4 UAT and Go-Live

System Integrator will assist in successful completion of User Acceptance Testing (UAT) and audit of the Hardware on the completion of the roll out and will submit a report for the same. The Application vendor along with assistance of network, Data centre and Hardware provider will integrate the hardware including the LAN, system software and application software and commission the whole project. The DDA/PMU shall conduct User Acceptance Testing on receipt of intimation of commission of the whole project from the bidder. Only after the acceptance of UAT reports by DDA, the entire infrastructure would be deemed to have been commissioned. After the successful commissioning of the project, the system would be

declared as Go-Live and enter into O&M phase and the selected bidder would also be issued a Go Live Report by DDA. Hardware vendor shall also provide following documents to the DDA

a. Installation Manuals
b. Transferring the ownership of all hardware & software procured.
c. All licenses & support related documents should be in the name of DDA.

1.4.5 Operation and Maintenance Phase

The selected Bidder is responsible for the day to day maintenance of the system for the entire period of Contract. For the IT Infrastructure procured as part of this RFP, the selected Bidder will be responsible for smooth Operations and Maintenance for the entire duration of the contract and shall provide

a. Onsite Warranty support
b. Onsite Periodic and AMC support including repair and replacement
c. Annual Technical Support (ATS) for all the licensed software provided by the bidder
d. Providing Help desk support with Escalation matrix for registration of complaints related to the IT Infrastructure and software procured through this procurement by DDA

1.4.6 Post Implementation Services

An indicative list of activities and nature of support to be provided is mentioned below:

1. System Administration and Trouble Shooting
   a. Repair or replace infrastructure deployed for this Project, either directly or through a third party warranty provider depending on the case
   b. Replace component due to technical, functional, manufacturing or any other problem with a component of the same make and configuration. In case the component of same make and configuration is not available, the replacement shall conform to open standards and shall be of a higher configuration and shall be approved by the Department
   c. 24 x 7 comprehensive onsite support arrangement for duration of the contract with all the OEM for respective components shall be provided.
2. MIS Reports and Incident Reporting

   The following is an indicative list of MIS reports to be submitted by the bidder post go-live. The selected Bidder shall also draw an exhaustive list of reports along with DDA. Bidder shall submit the reports on a regular basis in a mutually decided format. Bidder shall submit 1 hard copy and 1 soft copy of each of the reports. Indicative list if provided below:

   i Asset modification report at the DDA office locations sites and datacentre locations.
   ii Log of preventive / break-fix maintenance undertaken.
   iii Asset database report and Asset Audit report

3. Overall

   a. Undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any incidents) and carry out the necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours of DDA unless inevitable and approved by the *DDA*
   b. Undertake reactive maintenance (any corrective action, maintenance activity that is required post the occurrence of an incident) that is intended to troubleshoot the system with sufficient teams

1.4.7 Warranty Support

As part of the warranty services BIDDER shall provide:

a. BIDDER shall provide a comprehensive warranty and BIDDER needs to ensure that there is no downtime due to failure of Hardware and expired warranties. BIDDER shall obtain the requisite product warranty from OEM on all licensed software, computer hardware and peripherals, networking equipment and other equipment for providing warranty support to DDA.
b. BIDDER shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP.
c. BIDDER must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
d. BIDDER shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
e. Mean Time between Failures (MTBF): If during contract period, any equipment has a hardwarefailure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the BIDDER at no cost to *DDA*.
f. DBMS (Database Management System), EMS (Enterprise Management System), other products deployed as part of this project by the software vendor will require proper arrangements of BIDDER with OEM.
g. During the contract period BIDDER shall maintain the systems and repair / replace at the installed site, at no charge to DDA, all defective components that are brought to the BIDDER's notice.
h. Warranty should not become void, if DDA buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the BIDDER.
i. Warranty will not become void if any hardware added is connected to external ports and not installed within the machine.
j. The BIDDER shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.

k. BIDDER shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

l. The BIDDER shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

m. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

n. The BIDDER shall develop and maintain an inventory database to include the registered hardware warranties.

1.4.8 Asset Management

The selected Bidder will perform the following asset management functions with respect to the infrastructure deployed at various locations:

a. Take periodic stock of, review physical inventory and maintain stock registers of hardware at all locations covered under this Project. The selected Bidder would maintain stock registers as per format agreed with the *DDA*

b. Maintain documentation of the hardware assets, maintain asset Information for all Project locations, on parameters to be mutually agreed between the *DDA* and the selected Bidder, which shall include details like -

   i Product type, model number, version number

   ii Manufacturer

   iii Office location

   iv Maintenance status, etc.

c. Update or correct the asset information following any new installations, movement, addition, or change performed by the selected Bidder.

d. Produce periodic reports and machine readable files in agreed upon format pertaining to some or all of the asset information.

e. Restrict movement of server/equipment/items in or out of SDC or any other location under the Project without prior permission from the *DDA*

1.4.9 Knowledge Transfer

1. At the end of the Contract period, the selected Bidder will be required to provide necessary handholding and transition support to designated staff or any other agency that is selected for maintaining the system post the Contract with the selected Bidder. The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for the ITInfrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.
2. Knowledge Transfer is an integral part of the scope of work of the selected Bidder. This will have to be done even in case the Contract with the Bidder ends or is terminated before the planned timelines.

Please note that this is only an indicative list. Any other activity, over and above these, as may be deemed necessary by the selected Bidder to meet the service levels and requirements specified in this Contract are also required to be performed by the selected Bidder at no additional cost.

1.5 Network Design, Procurement, Deployment, Operations and Maintenance Services

DDA intends to engage reputed Service Provider for providing services for following three major activities:

1. Complete managed CPE TO CPE, IP MPLS VPN Services at all DDA locations / offices.--(The MPLS – Multi Protocol Label Switching - service includes network designing, providing all related network hardware on lease for connectivity, last mile, bandwidth, installation, configuration, hardening, maintenance support, integration with LAN/WAN, proactive monitoring and reporting, change management, migration, training and helpdesk etc., with SLA binding the Bidder to uptime (as indicate in this RFP) and application/service quality commitments.
2. DDA proposes to procure dedicated internet link at its outsourced Data Centre at Delhi/Noida/ &Disaster Recovery Centre at Mumbai/Bengaluru/Hyderabad/Chennai.
3. Campus wide LAN set up including laying of Optical Fiber, structured cabling, installation of 24 / 48 port Network Switches at all the DDA office locations.

The purpose behind issuing this RFP is to invite technical and commercial bids for selection of service provider for providing IP MPLS VPN connectivity at all locations/offices. DDA proposes to procure dedicated internet link at its outsourced Data Centre at DR Site & all the site offices. Broad scope of work is mentioned below

a. It may also be noted that all the activities in the IT operation are subject to audit /inspection by Security Auditors. Selected Bidder must take same into consideration while delivering the desired services.
b. The selected Bidder to provide multiple CoS(Class of Service)for real time traffic / non-real time traffic /business traffic. The selected Bidder shall undertake maintenance of Network equipment such as MPLS Routers, Network Switch at all locations/offices of DDA. The selected Bidder should be able to extend IP MPLS VPN to any new DDA locations/offices and shall be scalable to add new sites as and when required by DDA, at the contracted rate.
c. DDA may ask the selected Bidder to upgrade bandwidth from the initial contracted value to higher/lower value based on operational requirements.
d. DDA may ask the selected Bidder to shift the equipment and provide MPLS connectivity at any other location, in case of shifting of existing premises at any of the present or future DDA location as per contracted rate.
e. Shifting of premises - In the event of shifting of premises, order to this effect will be placed with the selected bidder. Bidder will carry out site-survey at the new location for feasibility of location for type of media and intimate DDA. On receipt of confirmation from the DDA, the Bidder to install and commission the link at the new location prior to shifting of office from old location. The vendor is required to implement and commission the location within 2 weeks from the date of order. The connectivity at the old location has to be dismantled and removed on the last day of shifting. The cost towards installation as per the contracted rate for the respective category will be applicable. Vendor may provide interim connectivity using MPLS USB dongles with high bandwidth upto 4 weeks from the date of order, if the commissioning is delayed.
f. In the event of non-commissioning of the link within 4 weeks from the date or order of shifting, penalty at the rate of 1% of the order value will be charged for every week delay, subject to a maximum of 10% of the order value.

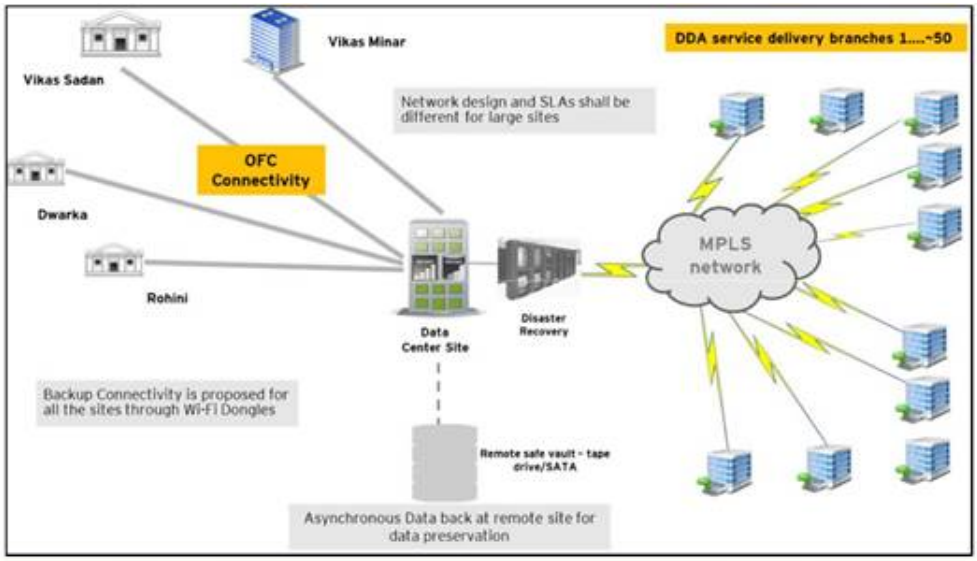
g. Shifting of equipment within premises/office - For shifting of equipment/lines (MPLS/ISDN) within the premises, vendor shall depute the concerned engineer/official within 24 hrs from the time of reporting of such requirement by the DDA. This is to enable smooth transition of network equipment and to ensure proper functioning of network connectivity at the new place of installation, in coordination with DDA's officials. Such shifting of equipment within premises/office shall be done at no cost to DDA, whatsoever.

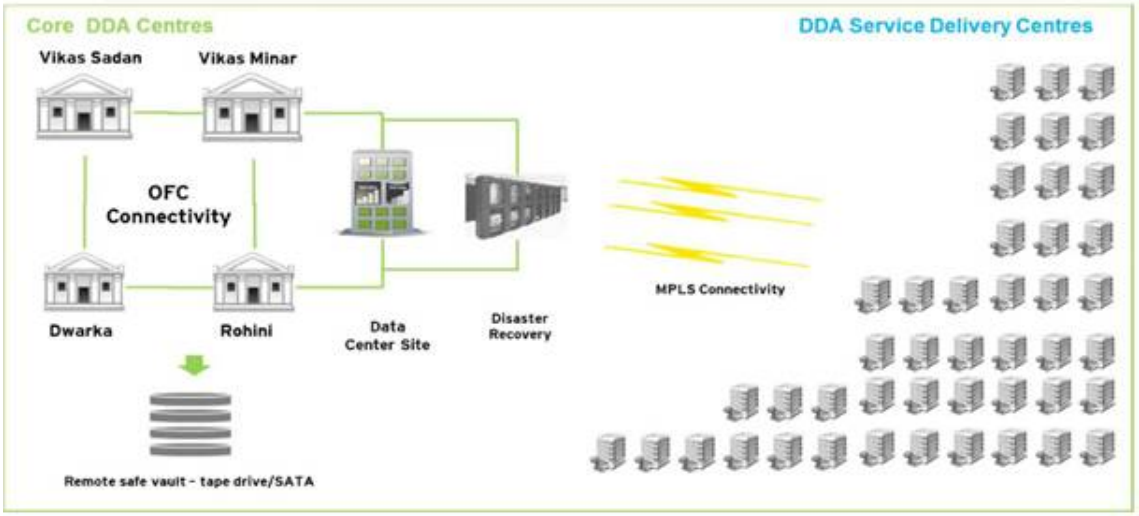
h. While providing a solution the bidder shall follow the "Key Design Principles" as mentioned in RFP volume 1. Irrespective of the option above chosen by the Bidder, the Bidder is required to meet all the requirements of this RFP including the activities listed, timelines and deliverables mentioned in this RFP.

1.5.1 Network Study and Design

1. Assessment of existing network.
2. The Network Service Provider shall create and maintain all project documents that shall be passed on to the DDA as deliverables as per the agreed project timelines. The documents created by the Network Service Provider will be reviewed by PMU and approved by DDA. Project documents include but are not limited to the following
   a. Detailed Project Plan
   b. Detailed Site Survey Report
   c. List of services, Service Definitions, Service Levels
   d. Network Architecture
   e. Detailed Bill of Materials
   f. Installation Reports
   g. Periodic SLA and Performance Monitoring Reports.
   h. Standard Operating Procedures
3. Bidder shall coordinate with DDA &and consortium members teams to resolve any problems encountered during and after rollout. All post implementation issues shall be documented and the necessary fixes / resolutions shall be implemented by bidder.
4. Bidder shall ensure necessary support is provided to resolve defects. Bidder shall document the defects / incidents encountered during this phase as well as document the resolution of the same.
5. The Network Service Provider shall submit a list of deliverables that they shall submit based on the methodology they propose. The Network Service Provider shall prepare the formats/templates for each of the deliverables upfront based upon industry standards and the same will be approved by DDA prior to its use for deliverables.
6. The Network service provider is supposed to provide connectivity to the sites including last mile connectivity. MPLS mesh based connectivity has been envisaged along with backbone on optical fiber at each floor/block level of the building (Vikas Sadan and Vikas Minar specifically) thereby ensuring fast and reliable speed.
7. Given the project of this size, bandwidth requirement at various locations/DDA offices, DC and DR at this stage is tentative. Depending upon the application solution proposed by the successful application development bidder and its utilization, bidder may be required to upgrade/size up the links. Such provisions shall be made by the successful bidder at no additional cost. Bidders are encourage to work in close coordination with application development team and DDA officials for finalizing the bandwidth requirements. However, it shall be the complete responsibility of the Network provider to size, commission and maintain the links.

8. Bidder is required to carry out survey for each site to study the exact requirements for setting up of LAN. Purpose of this exercise will be to understand the site layout & user's network requirements. DDA will do the necessary coordination required to carry out this activity.
9. LAN within all department offices including but not limited to IP addressing scheme, physical cabling, router/switch configuration, V-LAN configuration, load balancing configuration, and fail over mechanism. The selected Bidder should coordinate with the local department offices while designing and installing the LAN.
10. The bidder shall ensure that all networking equipment's required providing the LAN / WAN connectivity to meet the requirements of the Project is also to be provided by the selected bidder as part of this RFP. Any up gradation in bandwidth should not result in up gradation/change of any equipment after award of contract to the successful bidder. Bidders are therefore encouraged to carry out the site survey before proposing the solution
11. Bidder should plan for structured cabling for setting up Local Area Network. **The structured LAN cabling should be OEM certified for minimum 10 years**. Bidder may offer OEM certification of more than 10 years as well. Structured cabling should be done to meet the LAN requirements, and should not impact the availability & performance of the network, due to reasons including interference, Electro Magnetic Interference, Radio Interference, etc. and should meet the service levels defined in the RFP. Wherever required, the bidder is to use Shielded Twisted Pair ('STP') cabling.
12. Low-level design and configuration of the LAN and WAN including, but not limited to, IP addressing scheme, physical cabling, router/switch configuration, V-LAN configuration, load balancing configuration, and fail over mechanism to be provided by the Bidder.
13. The indicative requirements of network equipment to be supplied by Network Service Provider have been provide at Annexure 33, 1.2 of this RFP. However, the bidder may do his own sizing depending on the proposal.
14. An Indicative Network schemes are depicted below:





1.5.2 Preparation of Network Design

Detailed Design documents shall include:

1. Technical Architecture Document (Network, and Security)
2. The available IT network infrastructure available at DDA shall be a part of the document.

1.5.2.1 Sign off Deliverable/ Exit Criteria

The deliverable/exit criteria for network solution design shall be submission and subsequent approval of:

1. Detailed Project Plan

2. Detailed Site Survey Report
3. Installation Report vetted by DDA Officials

1.5.3 Connectivity Requirements for MPLS:

1. Any to Any connectivity required for all locations.
2. A separate MPLS VPN is to be created only for DDA network and in no way the VPN should be shared with other customers sharing the MPLS backbone. All routing at MPLS Backbone should be on Labels and no IP routing is acceptable. DDA MPLS Network must be accessible to DDA nodes only.
3. The LAN IP addresses in DDA offices where MPLS connectivity is proposed shall have to be provisioned & IP schema has to be decided by bidder in consultation with DDA & Application SI. The service provider to ensure that they configure MPLS
4. VPN link in such a way that there is minimal change in the IP scheme being currently used by DDA.
5. The last mile at DDA's Data centre & DR-site should have full redundancy through last mile connectivity from 2 different POPs of the service provider. If at some location Network Integrator provides last mile through other WAN service providers, the total responsibility of liaison, commissioning, maintaining the link including all commercials involved should be taken care by the bidder.
6. Last mile link should be on Fiber Optic using self-healing ring architecture for DDA Vikas Bhavan & Vikas Minar. For all other locations where ever OFC is not feasible, bidder may provision last mile link over Copper/RF.
7. If the last mile is on wireless, Service provider has to ensure that no other Radio equipment causes interference to wireless signals used for DDA's connectivity and the Radio equipment should not be able to trap the signals used for DDA's network.
8. All the equipment/devices installed must be IPv6 compliant and ready to handle IPv6 traffic.

1.5.4 Connectivity Requirements for Internet:

1. ISP should have fully resilient and self-healing network architecture on fiber medium, from the international gateway (either owned or hired) in India up to the international Points of Presence.
2. Bidder should propose 40 Mbps Internet link (1:1 uncompressed, unshared) at the Data Centre which can be upgraded up to 100 Mbps without any change
3. The bidder should provide Internet Link with last mile on Fiber and Ethernet handoff.
4. The bidder should provide at least 50 Public IP addresses (Class C) to DDA.
5. ISP should provide dedicated port for the connection (with no capping or rate limit).
6. Bidder should explicitly mention the make & model of equipment proposed to be supplied with the line from their end and the customer premise equipment required (if any) to be provided by DDA.
7. Average domestic latency should not be more than 100ms and Packet Loss should be less than 1% for the provided Internet Bandwidth.
8. Bidder must insure that the loop provisioning does not violate regulations as laid by Government of India/TRAI in respect of such links/networks.

1.5.5 Expected Performance:

S.No	Description	Measure
1	Availability / Uptime:	99.90% uptime
2	Latency [CPE to CPE]	Not more than 100 ms
3	Jitter	< 20 ms
4	Packet Loss	<= 1%
5	Mean time to Repair (MTTR)	<= 4 Hrs

1.5.6 Security

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

a The network shall provide end to end connectivity which includes the last mile connectivity

b All network equipment and type of connectivity shall provide robust security features and standards.

c There shall be adequate redundancies in the system so that connectivity is available for continuous access to data and resources. These redundancies will ensure that in case of outage of primary connectivity, users are able to access DDA systems with the help of redundant line.

d Network shall be designed without a single point of failure. System shall be designed to permit continued operations, albeit at reduced throughput, when a network fails in normal operations or in the event of a disaster.

e Networks shall be positioned for future growth in traffic and expansion of services such as data, voice and video.

f Network shall use switched multi-segment design with managed hubs.

g The system shall provide the capability to monitor all security-relevant activity. Establishing accountability and to detect security violations requires the capability to track security-relevant activity

h The system shall provide firewall technology, configured to protect the various network and host-based services of DDA.A firewall technology, configured to protect the various network and host-based services of DDA needs to be installed at external gateway. They provide well-established central points for protecting assets against intrusion and disruption. Tracking and monitoring of attempted security violations is critical to the prevention of damages to DDA assets.

i The system shall maintain accurate date and time.

j The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.

k The solution shall support advanced user authentication and data signing mechanisms including digital certificates.

l Perform risk assessment to identify the most important computers to protect. Computers that provide critical IT functions such as email, administrative systems. Use a centralized system logging service to look at patterns of unusual activity. Use network scanning utility to create a profile for each computer identified in the previous step and

   a. Disabling the network services that are not needed

   b. Running a host-based firewall to block unwanted network traffic

m 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.

n The proposed solution should be able to monitor security and intrusions into the system and take necessary preventive and corrective actions.

o The proposed solution must provide ACL objects and a security model that can be configured for enforcement of user rights

l) The proposed solution should be designed to provide for a well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.

m) Exception Management shall take care of the various exceptions that might arise out of the system. These exceptions shall be captured and managed providing suitable abstraction to the user.

n) The overarching requirement is the need to comply with ISO/IEC 27001 standards of security.

1.5.6.1 Sign-off Deliverables / Exit Criteria

Network Connectivity report signed off by PMU / DDA stating DC, DR, and all DDA offices have been connected

1.5.7 Scalability:

One of the fundamental requirements of the proposed network is its scalability. The architecture should be scalable without any architectural or equipment change and should be horizontally and vertically scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance for at-least four years from the date of deployment.

1.5.8 Network Monitoring System (NMS)

1. NMS solution shall be provided and a dedicated dashboard for monitoring the entire DDA's asset is to be established and maintained.
2. NMS and helpdesk console shall be provided wherein the bidder need to configure troubleshoot tickets related to LAN, MPLS Links and Internet links;
3. The bidder will have to deploy skilled helpdesk agents to provide resolution to the tickets being raised by web/email/phone call.
4. SLA monitoring and reporting.
5. Indicative SLA reports which are to be made available by the bidder on a web based system online for the DDA includes:
    a. Network (at HQ and ZO – project locations etc) availability
    b. Incidents report and Ticketing dashboard

1.5.9 Documentation

Bidder shall submit necessary documentation as below

1. LAN design - Address total LAN node requirement (e.g. conduct survey & prepare list of nodes locations within the rooms), modular with provision for easy additions, meet all the networking requirements, capable for data, use latest Gigabit fiber technologies for backbone & edge.
2. IP Schema - should prepare LAN IP addressing scheme, proxy & antivirus requirements, create in building VLAN for segregation between users, address all the LAN security issues, list civil & electrical requirement for Server room & active devices, list power requirements, fire safety, Bill of material of LAN active devices .
3. Structured cabling installation - cable routing on building blueprint / plan with scales & distances , integration of existing cabling infrastructure if required, identification of existingcable risers and equipment closets to be used, labelling plan for cabling infrastructure, marking & identification of entire LAN infrastructure , creation of separate cable trays / pathways / raceways if required , documentation required to be handed to building administration for safe keep of cabling infrastructure, Bill of material of LAN passive devices.
4. Commissioning , testing & documentation for maintenance – strategy for phased wise installation & commissioning of LAN , Testing & certification of LAN components & cablinginfrastructure, tools & manuals required for maintenance, suggest list items to stocked as spares for immediate fault rectification , schedules for periodic onsite maintenance of items / servers

1.5.10 Requirement of LAN at DDA Offices

1.5.10.1 Scope of Work, deliverables for LAN

1. Survey and Network Design Document
    a. Survey of all the Offices of DDA as given in Annexure 1 and prepare a survey report and detailed Network Design document.
    b. Network Design Document must include

c. Details of existing Networking infrastructure.

d. Detailed network design of the offices showing the deployment of switches and other components and the IP addressing schemes to be implemented in the DDA offices including CAT 6 connectivity, Fiber connectivity & MPLS & Internet connectivity.

e. Office / Location wise Deployment and Installation plan for CAT 6 connectivity, Fiber connectivity, MPLS & Internet connectivity.

1.5.10.2 Supply, Installation, Integration and Commissioning

1. Supply of products.-The Successful bidder shall:
   a. Supply all the items required for LAN (such as Optical Fiber cable, Patch panel, LIU, Switch etc.) and provide onsite comprehensive OEM warranty as per warranty (Terms & Conditions) for all the items supplied and installed.
   b. Supply any other equipment (like Screws, clamps, fasteners, ties, anchors, supports, grounding strips, wires, termination kits etc.) required for completing installation.
2. The selected Bidder is responsible for installation and configuration of the entire network infrastructure set-up
3. The selected Bidder will ensure that the reports for monitoring of SLAs such as system uptime, performance, etc. are generated automatically from the system and the applicable penalties are calculated as indicated in the RFP.
4. Installation, integration and commissioning of the Local Area Network (LAN) at all the offices of DDA. This shall include structured cabling, active and passive components of LAN at offices
5. Supply, Installation, configuration and commissioning of Switches& all the equipment and obtaining installation completion and commissioning certificate (Sign-Off) for all Implementation locations from the respective nodal/designated officer.
6. Preparation and submission of detailed User Acceptance plans (UAT)/ schedules/ procedures/ formats. All the costs towards testing & commissioning to be borne by the successful bidder.
7. Documentation: The successful bidder should submit following deliverables
   a. Delivery challans and installation certificate with hardware configurations.
   b. Shall submit a detailed Network Design Report containing following
      i IP Addresses configured at different equipments (switches etc.)
      ii IP Addresses and other IP settings to be done by the DDA officials on their Computers, Laptops etc. once connectivity is terminated at the switch
      iii Policies deployed at the Switches

1.5.11 UAT and Commissioning

Network service provider will assist in successful completion of User Acceptance Testing (UAT) and audit of the system on the completion and will submit a Go-Live Report. The DDA/PMU shall conduct

User Acceptance Testing on receipt of intimation of commission of the whole project from the bidder. After the successful Installation & commissioning of the project, the system would be declared as Go-Live and enter into O&M phase and the selected bidder would also be issued a Go Live Report by DDA. Network Service Provider should provide following documents to the DDA:

a. Installation Manuals
b. User manual (Role wise)
c. IT security policy
d. Access Control Policy
e. Incident Management Policy
f. Change management plan development

1.5.11.1 Sign-off Deliverables / Exit Criteria

Installation report signed off from concerned Officer nominated by DDA.

1.5.12 Stage 2 : Operation & Maintenance Support :

1.5.12.1 Overview of Post Implementation Services

An indicative list of activities and nature of support to be provided is mentioned below:

Coordinate with the network service providers to maintain smooth network operations and ensure uptime and performance requirements of the IT infrastructure as indicated in the RFP are met. The selected Bidder will be totally responsible for all networking equipment installed by him. Indicative list of activities to be performed by the bidders is:

1. Bidder should ensure that the network is available 24x7x365 as per the prescribed SLAs
2. Bidder should provide services for management of network environment to maintain performance at optimum levels.
3. Bidder would be responsible for attending to and resolving network failures and snags
4. Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
5. Configuration and backup of network devices including documentation of all configurations
6. Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers
7. Bidder would create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers for the DDA
8. Bidder should provide support as required to assist with hardware and software problem isolation and resolution in the LAN/WAN environment.
9. Bidder should be responsible for trouble shooting of entire network and hardware provided by him
10. Bidder should maintain LAN/WAN configuration data.
11. Bidder should ensure smooth routing of network traffic to the DR site in case of disaster / drill.

12. Supplier shall provide comprehensive Maintenance & Support Services for supplied Hardware and software infrastructure, etc. This involves comprehensive maintenance of all component covered under the contract, including repairing, replacement of parts,modules, sub-modules, assemblies, sub-assemblies, spares part, updating, security alerts and patch uploading etc. to make the system operational.
13. Bidder shall provide details of service engineers at specified locations during commissioning of the Local Area Network (LAN).
14. The selected Bidder is responsible for the day to day maintenance of the system for the entire period of Contract. For the IT Infrastructure procured as part of this RFP, the selected Bidder will be responsible for smooth Operations and Maintenance for the entire duration of the contract and shall provide
15. Providing Help desk support with Escalation matrix for registration of complaints related to the IT Infrastructure procured through this RFP by DDA
16. Reinstallation/ reconfiguration of Switches, installing latest firmware and upgrades.
17. DDA officials may lodge complaints by any mode i.e. phone, e-Mail, post. Bidder shall provide a complaint/ ticket number for each complaint and has to resolve the problem within the stipulated period as mentioned in this RFP. Complaints shall be logged with the service engineers deployed at different locations.
18. The network service provider would be required to position resources to provide technical support at each of the office during the roll out period. This would be essential to ensure sufficient handholding is provided to department personnel in the various offices to manage the system after the end Contract Period

1.5.12.2 Help Desk and Trouble ticket management system

1. The selected Bidder as part of provisioning support for Department users at each location and the DC will setup centralized helpdesk and coordinate with the respective OEMs of the IT Infrastructure deployed at DC and the Department offices for trouble ticket resolution within the stipulated timeline.
2. The network service provider shall use helpdesk management system (to be provided by DDA) for Helpdesk Call management and SLA reporting. The flow of events at the service desk should be:
    a. Event is triggered and forwarded to service desk.
    b. Service desk submits and updates the trouble ticket.
3. Tasks expected:
    a. Ticket mapping and allocation: According to the severity, the ticket should be given the priority level. Also it should map the ticket to the appropriate personnel for the resolution.
    b. Updating the status: Update the status of ticket.
    c. It should be able to log and escalate user interactions and requests.
    d. It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
    e. Historical report indicating number of calls, time to resolve, status etc. for a specified period of time.
4. During and after the end of the project period, the Network Service Provider shall refrain from canvassing DDA and any of its associates with any claim for employment of bidder's personnel deployed under the project.

1.5.12.3 Warranty Support

As part of the warranty services Network Service Provider shall provide:

1. Network Service Provider shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment,accessories etc. covered by the RFP to ensure that there is no downtime due to failure of Hardware and expired warranties.
2. Onsite Periodic and AMC support including repair and replacement
3. Network service provider shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
4. During the warranty period Network Service Provider shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost to the *DDA* in case the procured hardware or software is not adequate to meet the service levels.
5. Mean Time between Failures (MTBF): If during contract period, any equipment has a hardwarefailure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the Network Service Provider at no cost to *DDA*.
6. Warranty should not become void, if *DDA* buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the Network Service Provider.
7. Warranty will not become void if any hardware added is connected to external ports and not installed within the machine.
8. The network service provider shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of hardware supplied and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.
9. Network service provider shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
10. The Network service provider shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
11. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
12. The Network service provider shall develop and maintain an inventory database to include the registered hardware warranties.

1.5.12.4 Annual Technical Support

As part of the ATS services Network Service Provider shall provide:

1. Network Service Provider shall maintain data regarding entitlement for upgrades, enhancements, refreshes, replacements and maintenance for the equipment provided

2. If the Operating System or additional copies of Operating System are required to be installed/ reinstalled / de-installed, the same should be done as part of ATS.
3. Network Service Provider should carry out any requisite adjustments / changes in the configuration for implementing different versions of Firmware/OS.

1.5.12.5 Configuration Management Services:

1. The vendor shall maintain complete configuration (in hardcopy & softcopy) details of all the items supplied and installed by him.
2. The vendor shall define change management procedures and also ensure that no unwarranted changes are carried out. Any changes shall be incorporated with prior approval of the purchaser.
3. The network service provider shall do proper version management of these configurations as they are bound to change from time to time.

1.5.12.6 Asset Management

The selected Bidder will perform the following asset management functions with respect to the infrastructure deployed at various locations:

a. Take periodic stock of, review physical inventory and maintain stock registers of hardware at all locations covered under this Project. The selected Bidder would maintain stock registers as per format agreed with the *DDA*
b. Maintain documentation of the hardware assets, maintain asset Information for all Project locations, on parameters to be mutually agreed between the *DDA* and the selected Bidder, which shall include details like -
    i Product type, model number, version number
    ii Manufacturer
    iii Office location
    iv Maintenance status, etc.
c. Update or correct the asset information following any new installations, movement, addition, or change performed by the selected Bidder.
d. Produce periodic reports and machine readable files in agreed upon format pertaining to some or all of the asset information.
e. Restrict movement of equipment/items in or out of any/all locations under the Project without prior permission from the *DDA*

1.5.12.7 Other:

1. The entire Hardware as supplied under the project should be interoperable. In case any additional device/ software are required for interoperability, the same shall be provided, installed and maintained by the bidder at no extra cost for entire warranty period.
2. To provide all patches and updates during the entire warranty period.
3. To obtain Installation certificates from all locations and submit it to purchaser

1.6 State-of-the-Art Record Room Management (Asset Management) managed by Documentalist / Librarian

Record Room Management System is required to be set up at DDA with 50 Record Rooms in different location within Delhi. The approximate room size may be of 20X15X10 feet with appropriate number and size of Non corrosive Rolling Record Box Storage Racks with Serial number Identification board as shown in the picture. There will be about 5, 00,000 Files (Five Lakhs) to reside in the record rooms. The low-profile rail required to be used with the Rolling Record Box Storage Racks for easy operations.

DDA envisages to create a "Digital Library" using dovetailing Digital technology, Internet connectivity, and physical content (Files). A digital library is being built around specific repository software. The best-known examples of this software are DSpace, Koha and e-Granthalaya software products.

Digitization through scanning and creation of Digital Library will be as per the standards of" Digital Preservation and Information Life Cycle Management" of the Ministry of Electronics and Information Technology, under its National Digital Library Project.

Presently Files are physically kept in the record rooms or in sections in Almirahs/ racks. If some File is lost or misplaced there is no way to track it. A new file is reconstructed by taking some documents from the applicant. Some files have already been scanned. There should be a Centralized Digital Library (Archival) with High speed Computer Servers with SAN storage of appropriate Tera bytes storage;document management System (DMS) and retrieval software;scanning and archiving of all files and important documents are in the DMS. Files can be easily constructed with already scanned files and made available through Online File Movement System software (e.g. eOffice of GOTS).

Please also refer to FRS (Annexure-34) – Document Management Solution (DMS)and also the existing Document Scanning Policy of DDA wherein details of requirements are specified.

1.7 RFID File Tracking System

RFID (Radio Frequency Identification) based File Tracking System (FTS) is ideal solution to track the important documents within the offices.

The File Tracking System (FTS) enables users to automate management of physical record data and improve the productivity without any inventory errors.A wide range of enterprises rely on files and folders, and records that must be accurately tracked and located, including Government agencies.

RFID File Tracking Systems are required to reduce employee time spent maintaining and managing hundreds or thousands of files within a DDA. Many businesses currently use basic methods to manage files, such as alphabetical filing, color-coded filing, or barcodes. RFID file management systems have become increasingly popular because they give employees enhanced visibility, while freeing up time previously spent on inventory counts or searching for lost documents.

The System must be able to for Read, Record, and Report on Real Time Basis where ever the file is and must capture the movement and journey of File with in the office. The system

should be able to capture the entry and exit of Files with in section, within premises and then entry and exit of the premises through hand held scanner or Mobile App.

The System Specification includes (a) Readers: Desktop Readers, Wallmount Readers, Handheld Readers; (b) Passive UHF RFID Labels, (c) Central Server Hardware, (d) Centralized Data Management Server (Manages all Readers, Collect & Process Data, Create Alerts, Server data to Web based File Tracking Software) and (e) Web based Software for File Tracking Software. (Runs on same server).

RFID hardware products for library are required to be compatible with global protocols such as SIP2 ,NCIP, ISO 18000-3, ISO 15693, ISO 14443A & ISO 28560 (Part 1, 2 & 3).

Please also refer to FRS (Annexure-34) wherein details of requirements are specified.

1.8 Setup of Nagrik Suvidha Kendra

NAGRIK SUVIDHA Kendra has been conceived to facilities citizen by capturing the input at a single point, defining a specified delivery date depending upon the type of service and accepting fee charges at the counter itself/online payment. The objectives of NAGRIK SUVIDHA KENDRA Project are as follows:-

i To provide service level convenience to the citizens

ii Re-engineering of Government Processes to provide quality & timely services to citizen;

iii To integrate NAGRIK SUVIDHA KENDRA Back-end Services (SUBS) with front-end to reduce the time of delivery.

iv Linkage with Web based Citizens IT Interface (WebCITI) or Dialup base Citizens IT Interface (DialCITI) to know the latest information about their service.

As of now, the project is being executed only to facilitate the receipt of application forms for conversion of Residential/Commercial Properties allotted by DDA from Lease Hold to Free Hold. In future, the project shall be extended to provide the other facilities like receipt of all types of application forms viz mutation, change of address, subletting permission, mortgage permission etc.

1.8.1 How NAGRIK SUVIDHA KENDRA Works?

The citizen approaches NAGRIK SUVIDHA KENDRA Queue Counter and gets the Queue Token number.

He waits for some time till his token number is displayed on the screen. On his turn at NAGRIK SUVIDHA KENDRA Service Counter, he files his application.

She/he is issued a receipt cum token number, which specifies the date of delivery of services. Each type of service has a pre-defined delivery time and system automatically calculates the service delivery date.

All kind of payments for the fees etc., can be made at the NAGRIK SUVIDHA KENDRA counter as well as online payment mode. This further saves the inconvenience of the citizen caused to visit either bank or treasury office to deposit such payments. The application/case is then sent to the branch for action.

In between the citizen can track the case with the help of Email ID, Mobile No. furnished by the applicant in the application form as well as the Web site of DDA.

The delivery of documents/processed case is made on the specified date. The delivery of the documents is also from NAGRK SUVIDHA KENDRA Delivery Counter and not from the branch. This way the branches are able to concentrate on the backend work rather than attending to the citizens and this further helps in improving government services and the citizen are freed from inconvenience/harassment.

With this process, all applications received are recorded and monitored against the delivery due date, branch-wise. Computerized print, placement of processes has improved the quality of service. NAGRIK SUVIDHA KENDRA Software provided the facility of online application also. The operators are available on the counters for the prescribed timings on all working days from 10.30 A.M. to 4.30 P.M. so as to easily accessible to the citizens.

As of now, 4 Nagrik Suvisha Kendras are operational. Another 22 Nagrik Suvidha Kendras are expected to be establish under this Project.

1.9 Setup of Mobile Van Nagrik Suvidha Kendra

The functions of Mobile Van Nagrik Suvisha Kendra are of same as that of Nagrik Suvisha Kendras but the Van fitted with the relevant ICT Infrastructure and Internet Connectivity will move from one DDA Colony to another depending upon the demands from the Residents. These Mobile vans will be equipped with computers / laptops, printers, data cards (for internet access to DDA websites and other related websites), etc., and manned by appropriate Manpower. The Capex and Opex are to be included in the Financial Bid.

Under this Project, it is expected to operate **about 7** State –of –the –Art Mobile Van NSKs in Delhi.

1.10 Setup of Internet Information Kiosks (IIK)

An interactive kiosk is a computer terminal featuring specialized hardware and software that provides access to information and applications.

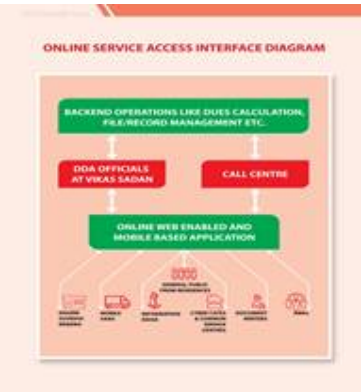
DDA desires to establish about 27 such Internet Information Kiosks (one in each SDM Office, 3 SDM offices in each District and there are 9 Districts in NCT of Delhi) in Delhi to facilitate DDA Customers to register their properties in SDM Offices in Delhi, facilitating access to DDA's Information and Applications.

These Internet kiosks will be from "hacker activities". Vendors who provide Internet kiosks are encouraged to use special Internet kiosk software and management procedures to reduce exposure to liability.

Such IIK will be of free standing interactive internet information IP phone kiosk with metal keyboard, Information Kiosk features.

1.11 Establishing fully Computerized Call Centre (CCC)

This CCC will be operational on all 07 days with at least 05 operators with DIALER/ EPABX facility and IVR.



1.12 Roles and Responsibilities of the Successful/ Selected Bidder

1. Shall deliver, install and maintain all Goods and Services in the given timelines and as per the SLA given in the tender document;
2. Should co-ordinate with local DDA Officers and all the required stakeholders to resolve any issues related to project.
3. Should timely escalate the issue with the DDA staff in case of any intervention, directions required from the DDA.

1.12.1 Indicative Bill of Material

Indicative bill of materials is specified in Annexure 33.All the supplied Hardware/ Software should be Interoperable, IPv6 ready and in compliance with the policies/ guidelines issued by DIT, GoI in this regard. Also, **the bidder is to quote/ propose only one make/ model against the respective item.**

All the equipment to be hosted at DDA offices should be rack mountable and the selected bidder shall have to mount the equipment in Rack(s) with required accessories/ cables/ screws etc. All the supplied Hardware/ Software should be IPv6 ready from Day 1 & must support Dual Stack.

Bidder shall include all the components (other than mentioned above) that are required to make the solution complete.