No: IE/_02_/_03_/24-25

RFQ

for providing

Design, Development, Hosting and Maintenance of Dashboard and Mobile Application

23rd January 2025

National Productivity Council
(Under Ministry of Commerce & Industry, Govt. of India)
Utpadakta Bhavan, 5-6 Institutional Area,
Lodhi Road, New Delhi-110003

Table of Contents

SECTION 1 - INVITATION TO BID

The National Productivity Council (NPC), operating under the Ministry of Commerce and Industry, Government of India, seeks proposals from qualified software solution providers for an ambitious digital initiative supporting the National Food Security Act (NFSA) 2013. This project encompasses the design, development, deployment, testing, security audit, hosting, and maintenance of a comprehensive Dashboard and Mobile Application system.

The selected agency will develop a system capable of facilitating nationwide surveys across all states and union territories. This system must efficiently manage data collection from approximately 50,000 beneficiaries annually through a mobile application, with subsequent integration into a centralized dashboard for analysis and reporting.

The scale of this initiative requires robust infrastructure capable of supporting approximately 500 concurrent dashboard users and 150 field investigators conducting daily surveys. The system must maintain 24/7 availability for report access and downloads, ensuring uninterrupted service delivery. Furthermore, the solution must incorporate comprehensive data retention capabilities, maintaining accessibility and security for five years – three years during active operations and an additional two years for reference and audit purposes.

To ensure long-term value and sustainability, the selected agency will provide maintenance and support services for three years following successful deployment. This support phase will address ongoing requirements, system enhancements, and necessary updates while maintaining optimal performance and security standards.

The selection process will follow this schedule:

Milestone Event	**Date**
RFQ Issue Date	23.01.2025
Pre-Bid Meeting	30.01.2025
Technical and Financial Bid Submission Deadline	14.02.2025
Technical Bid Opening	To be informed
Technical Evaluation & Presentation	To be informed
Financial Bid Opening	To be notified to qualified bidders

Interested agencies can download the tender document from the NPC website (www.npcindia.gov.in). For bid submission, agencies must download an official copy from the GeM Portal. All future communications, including corrigenda, addenda, and amendments, will be published on both the NPC and GeM/CPPP Portals. NPC will not distribute printed copies of the tender document.

Agencies should note that all costs associated with bid preparation and submission remain their responsibility. NPC bears no liability for these costs, regardless of the bidding process outcome. Early registration on the GeM/CPPP Portal is strongly recommended to avoid delays during bid submission.

Contact Details for Queries:

Director and Group Head (IE)
National Productivity Council
Utpadakta Bhawan Lodhi Road, New Delhi 110003
Tel: 011-24607367, 24607377
Email: npciehq@npcindia.gov.in

This document is non-transferable, and NPC reserves the right to modify any aspect of the selection process prior to the bid submission deadline. Any such modifications will be communicated through the official portals mentioned above.

The evaluation process will consider both technical expertise and financial viability, ensuring the selected agency possesses the necessary capabilities to execute this critical national initiative successfully. We encourage responses from organizations with demonstrated experience in developing and maintaining large-scale, multi-lingual digital solutions for government projects.

SECTION 2 - BACKGROUND AND OBJECTIVES

The National Productivity Council requires a comprehensive digital solution for concurrent evaluation of the National Food Security Act (NFSA) implementation. This system must support large-scale data collection through mobile applications and provide advanced analytics through a centralized dashboard.

The system will handle an annual survey volume of approximately 50,000 beneficiaries, with data being collected by more than 200 field investigators and analyzed by 500 dashboard users across various administrative levels.

System Architecture Requirements:

The solution requires three primary components:

1. A mobile application supporting offline data collection with automatic synchronization capabilities. The application must facilitate structured surveys, capturing text responses, photographs, GPS coordinates, and digital signatures. Field investigators should be able to work offline in remote areas and synchronize data when connectivity becomes available.

2. A web-based dashboard providing real-time analytics and reporting capabilities. The dashboard must support concurrent access by 500 users across different administrative levels, each with specific data access permissions and analytical capabilities based on their role.

3. A secure server infrastructure, to be procured and maintained by the selected agency in accordance with Government of India guidelines. While the agency will manage this infrastructure throughout the contract period, ownership will vest with NPC.

User Access Framework:

The system must support five distinct administrative levels, each requiring specific interfaces and capabilities:

1. National Level Access: Complete data visibility and system administration capabilities
2. Zonal Level Access: Multi-state data access and comparative analysis tools
3. State Level Access: State-specific data management and report generation
4. District Level Access: Local data validation and field operation management
5. Field Investigator Access: Data collection and primary validation capabilities

Data Management Requirements:

The system must maintain data accessibility and integrity for five years, divided into:

- Three years of active operations with full system functionality
- Two years of extended data retention with continued access to historical data

Performance Requirements:

The system must maintain:

- 99.5% uptime during operational hours
- Response time under 2 seconds for standard operations
- Support for 500 concurrent dashboard users
- Offline functionality for mobile application users
- Real-time data synchronization when connected

Infrastructure Requirements:

The selected agency will be responsible for:

- Server procurement following government guidelines
- application hosting Server to be procured from MeITY empaneled Cloud Service Providers (CSP)
- Infrastructure setup and maintenance
- Security implementation and updates
- Backup and disaster recovery systems
- Performance monitoring and optimization

All infrastructure components, including hardware, software licenses, and security certificates, will be owned by NPC while being managed by the selected agency during the contract period.

Expected Data Types:

The system must handle various data formats including:

- Structured survey responses
- GPS coordinates
- Video, Photographs and digital signatures
- Timestamped transaction records
- User activity logs
- Performance metrics

Security Requirements:

The solution must implement:

- End-to-end data encryption
- Role-based access control
- Multi-factor authentication
- Audit logging
- Regular security updates

This digital solution will serve as the primary tool for evaluating NFSA implementation effectiveness across India. The selected agency must ensure robust system architecture, reliable performance, and comprehensive security while maintaining flexibility for future enhancements.

SECTION 3 - SCOPE OF WORK

The scope encompasses the complete system development lifecycle, from requirement analysis through deployment and maintenance, including data retention period support. The entire implementation must comply with Guidelines for Indian Government Websites (GIGW) and undergo security audit by CERT-IN and STQC empanelled agencies.

Development Phase (28 Days):

The initial development phase begins with requirement analysis and design documentation. During the first 15 days, the agency must conduct detailed requirement gathering sessions with NPC stakeholders to understand system functionality, data flows, and integration needs. This phase culminates in comprehensive System Requirement Specifications (SRS) and Functional Requirement Specifications (FRS) documents.

The subsequent development period of 21 days focuses on creating the mobile application and dashboard components. The mobile application development must prioritize offline functionality, data validation, and synchronization capabilities. Concurrent dashboard development should establish the analytics framework, reporting mechanisms, and user management systems.

The final week focuses on integration testing, security implementation, and preparation for deployment. During this period, the agency must also initiate the security audit process with CERT-IN and STQC empanelled agencies.

Infrastructure Setup:

The agency must procure and configure server infrastructure according to government guidelines. This includes establishing three distinct environments:

- Development Environment: Supporting continuous development and testing activities with configuration management and version control systems.
- Staging Environment: Enabling user acceptance testing, performance validation, and pre-production verification with data sets comparable to production volumes.
- Production Environment: Implementing high-availability infrastructure with automated failover capabilities and real-time monitoring systems.

Application Components:

Mobile Application: The system requires native applications for both Android and iOS platforms. These applications must support:

- Offline data collection with automatic synchronization
- Multi-language interface and data entry
- GPS location tracking and photo capture
- Digital signature collection

- Real-time data validation
- Secure data storage

The agency must implement and maintain:

- Voice recognition services for all supported languages
- Translation services with high accuracy requirements
- Custom input control mechanisms
- Regular updates to language models
- Performance monitoring for voice and translation services

Dashboard Interface: The web-based dashboard must provide:

- Role-based access control
- Real-time data visualization
- Custom report generation
- Performance monitoring
- User management capabilities

Database Implementation:

The system requires a robust database architecture supporting:

- Multi-language data storage
- Data Encryption/ Protection as per Cyber Security Guidelines
- High-volume transaction processing
- Data versioning and audit trails
- Automated backup mechanisms
- Data archival processes

Security Implementation:

Security measures must address:

- Data encryption at rest and in transit
- Multi-factor authentication
- Role-based access control
- Security logging and monitoring
- Regular vulnerability assessments

Training and Documentation:

The agency must provide:

- System administration documentation
- User operation manuals

- API documentation
- Database schemas
- Security implementation details

Maintenance Phase (3 Years):

Throughout the operational period, the agency must deploy one qualified technical resource onsite at NPC headquarters in Delhi. This resource must possess a minimum of seven years of relevant experience in dashboard and mobile application development, along with BE/B.Tech/MCA or equivalent qualification. The onsite resource will serve as the primary technical point of contact, responsible for day-to-day system maintenance, user support, and coordination with the offshore development team.

The onsite resource must be equipped with necessary development tools, including laptop and required software licenses, provided by the agency. This resource will work during standard office hours (9:30 AM to 6:00 PM, Monday to Friday) and must be available for emergency support when required. Any replacement of this resource requires minimum 30 days notice and proper knowledge transfer, with NPC's prior approval.

During this three-year maintenance period, the agency through its onsite and offshore team must provide:

- System monitoring and optimization
- Bug fixes and security updates
- Performance tuning
- Feature enhancements as required by NPC
- First-level user support
- Regular system health reports
- Training for new users
- Documentation updates
- Full functioning of mobile application and dashboard 24/7 in all above-mentioned respects for 3 years

The onsite resource must participate in regular review meetings, provide status updates, and ensure prompt resolution of any technical issues. This resource should also assist in capacity building of NPC staff through knowledge transfer and training sessions.

Extended Data Retention (2 Years):

Following the operational period, the agency must ensure:

- Continued data accessibility
- System availability for report generation
- Security maintenance
- Backup management
- Technical support

Transition Support:

At contract conclusion, the agency must facilitate:

- Complete system handover
- Knowledge transfer
- Documentation updates
- Data migration support
- Training for new maintainers

Performance Requirements:

Throughout the contract period, the system must maintain:

- 99.5% uptime during operational hours
- Page load times under 2 seconds
- Support for specified concurrent users
- Data integrity and security
- Backup and recovery capabilities

The agency must provide regular performance reports and maintain detailed system logs for audit purposes. All modifications or enhancements during the contract period must undergo appropriate testing and security validation before deployment.

SECTION 4 - COMPREHENSIVE AUDIT

The agency must conduct comprehensive security audits through CERT-IN empanelled auditors annually throughout the contract period. These audits serve to verify system security, assess vulnerabilities, and ensure compliance with government regulations. The agency bears responsibility for both audit costs and subsequent remediation efforts.

Application Security Assessment

The annual audit must thoroughly examine all system components. For the web dashboard, this includes assessment of the frontend interface, backend services, and database systems. The mobile application audit must cover both Android and iOS versions, examining client-side security, data storage mechanisms, and communication protocols. All APIs require thorough security validation, including authentication mechanisms, data validation, and access controls.

The agency must ensure the audit covers encryption implementations for data at rest and in transit. This includes evaluation of key management systems, certificate handling, and secure storage practices. The assessment should verify proper implementation of multi-factor authentication, session management, and access control mechanisms.

Infrastructure Security Verification

The hosting infrastructure requires comprehensive security validation. This encompasses network configuration review, firewall rule assessment, and intrusion detection system verification. The audit must confirm proper implementation of security patches, system hardening measures, and access control mechanisms across all environments.

For cloud-hosted components, the audit must verify compliance with MeitY guidelines for government cloud deployment. This includes assessment of data localization, access controls, and security monitoring systems. The audit should validate disaster recovery mechanisms, backup procedures, and business continuity measures.

Data Protection Validation

The audit must verify protection mechanisms for all data types handled by the system. This includes validation of:

- Personal data encryption methods
- Access control implementations
- Data backup security
- Audit logging systems
- Data retention controls

The agency must conduct comprehensive testing of:

- Voice recognition accuracy across languages
- Translation accuracy and consistency
- Input control mechanisms
- Performance under various network conditions

Security Testing Requirements

The agency must ensure comprehensive security testing through:

- Source code security assessment
- Penetration testing of all interfaces
- Vulnerability scanning
- Security configuration review
- Access control testing

Each testing phase requires detailed documentation of findings and remediation measures. The agency must address all identified vulnerabilities according to their severity, with critical and high-priority issues requiring immediate resolution.

Compliance Verification

The audit must verify compliance with:

- CERT-IN security guidelines
- STQC requirements
- GIGW standards
- Data protection regulations
- Government cloud security norms

Documentation Requirements

The agency must maintain detailed audit documentation including:

- Test cases and methodologies
- Vulnerability assessment reports
- Remediation plans and timelines
- Compliance certificates
- Post-remediation verification reports

Audit Timeline Management

The agency should initiate the audit process two months before the due date, allowing adequate time for:

- Pre-audit preparation
- Security assessment
- Vulnerability remediation
- Compliance verification
- Certificate renewal

Continuous Security Monitoring

Between annual audits, the agency must maintain continuous security monitoring through:

- Automated vulnerability scanning
- Security log analysis
- Access control reviews

- Configuration assessments
- Performance monitoring

The monitoring system must generate alerts for security events, unusual activities, or performance anomalies. The agency must maintain detailed logs of all security incidents and resolution measures.

Post-Audit Requirements

Following each audit, the agency must:

- Address all identified vulnerabilities
- Update security documentation
- Enhance monitoring systems
- Implement recommended controls
- Update security certificates
- Provide immediate solutions to the problems identified in audit

The agency must maintain audit compliance throughout the five-year system lifecycle, including both the operational period and data retention phase. This ensures consistent security standards and data protection throughout the project duration.

SECTION 5- LIMITED AUDIT

5.1 Purpose and Scope

Beyond the annual comprehensive audit, the agency must conduct limited security audits through CERT-IN empanelled auditors in response to specific system changes. These targeted audits serve as crucial validation steps whenever significant modifications occur in the system's architecture, functionality, or security framework. The agency must engage a CERT-IN empaneled auditor different from the one performing the annual comprehensive audit to ensure fresh perspective and independent validation.

5.2 Audit Triggers

The need for a limited audit arises from four primary categories of system changes:

5.2.1 System Functionality Changes

A limited audit becomes mandatory when implementing new functionality or making major modifications to existing code. This includes:

- Addition of new system features
- Modifications to core business logic
- Changes to database structures
- Updates to data validation rules
- Modifications to processing workflows

5.2.2 Infrastructure Modifications

When undertaking changes to the hosting environment or system infrastructure, the agency must conduct focused security assessments covering:

- Migration to new hosting platforms
- Significant cloud configuration updates
- Network architecture modifications
- Security control implementations
- Performance optimization changes

5.2.3 Integration Updates

Changes to system integration mechanisms require validation of:

- New or modified API implementations
- Data exchange protocols
- Authentication mechanisms
- Security parameters
- Integration workflows

5.2.4 Access Control Modifications

Security validation becomes necessary when changing:

- Role definitions and hierarchies
- Permission structures
- Authentication methods
- Session management rules
- Security policies

5.3 Implementation Timeline

The agency must follow a structured timeline for limited audits:

Within 15 days of implementing changes: Initiate the audit process with selected auditor

Days 15-45: Complete the audit process including:

- Security assessment
- Vulnerability identification
- Risk analysis
- Initial findings report
- Remediation planning

Days 45-60: Address identified issues with priority-based resolution:

- Immediate resolution of critical findings
- Systematic addressing of all vulnerabilities
- Documentation of fixes
- Verification testing

By Day 60: Submit comprehensive compliance report to NPC detailing:

- Audit methodology
- Findings and resolutions
- Updated security posture
- Recommendations
- Compliance status

5.4 Quality Assurance Requirements

The audit process must maintain rigorous quality standards throughout its execution. The agency must ensure comprehensive testing coverage while minimizing impact on system operations. Performance monitoring during the audit should verify that security assessments don't adversely affect system availability.

5.5 Documentation and Reporting

The agency must maintain detailed documentation throughout the audit process. This documentation serves both immediate compliance needs and provides reference for future system modifications. Key documentation includes technical specifications, implementation details, test results, and remediation measures.

5.6 Responsibilities and Compliance

The agency bears full responsibility for:

- Audit execution costs
- Remediation implementation
- Documentation maintenance
- Compliance verification
- Status reporting to NPC

NPC reserves the right to request additional testing or validation if initial results indicate potential security concerns or incomplete remediation efforts. The system may return to normal operation only after verification of all security measures and NPC's acceptance of the compliance report.

SECTION 6 - INDICATIVE DELIVERABLES

6.1 Development Phase Documentation

The development phase requires comprehensive documentation establishing the foundation for system implementation. The agency must prepare and submit detailed requirement and design documents that clearly articulate system architecture, functionality, and implementation approach. These documents form the basis for development and future maintenance activities.

6.1.1 Requirement Documentation

The agency must deliver detailed requirement specifications including:

- System Requirement Specifications (SRS) detailing technical architecture, infrastructure requirements, and system interactions
- Functional Requirement Specifications (FRS) describing system behavior, user interfaces, and business logic
- Integration Specifications outlining data exchange mechanisms and API structures
- Security Requirements defining access controls, encryption standards, and audit mechanisms

6.1.2 Design Documentation

Design documentation must provide comprehensive technical blueprints covering:

- High-Level Design outlining system architecture, component interactions, and technology stack
- Low-Level Design detailing module specifications, database schema, and API contracts
- User Interface Design including wireframes, workflow diagrams, and interaction patterns
- Security Design specifying implementation of security controls and audit mechanisms

6.2 System Components

The agency must deliver fully functional system components developed according to approved specifications. These deliverables constitute the core system implementation.

6.2.1 Mobile Application

The agency shall deliver native applications for both Android and iOS platforms implementing:

The mobile applications must provide seamless operation in both online and offline modes, with automatic synchronization capabilities. The implementation must include comprehensive testing documentation and deployment guides for both platforms.

6.2.2 Dashboard Application

The web-based dashboard must deliver comprehensive monitoring and analytical capabilities through:

- Administrative interface for user and role management
- Real-time data visualization components
- Customizable reporting engine
- Performance monitoring tools
- System configuration interface

6.3 Infrastructure Setup

The agency must establish and document complete infrastructure implementation including:

Production Environment:

- High-availability server configuration
- Load balancing implementation
- Backup and recovery systems
- Monitoring and alerting setup
- Security control implementation

Development and Testing Environments:

- Configuration matching production specifications
- Development tools and frameworks
- Testing frameworks and automation tools
- Version control systems
- Continuous integration setup

6.4 Security Implementation

The agency must deliver comprehensive security implementation demonstrated through:

A safe-to-host certificate from CERT-IN empanelled agencies serves as validation of security implementation. The agency must maintain detailed documentation of all security measures and audit trails.

6.5 Training and Knowledge Transfer

The agency shall provide comprehensive documentation supporting system operation and maintenance:

Technical Documentation:

- System architecture and component documentation
- Database schemas and data dictionaries
- API documentation and integration guides
- Security implementation details
- Deployment and configuration guides

User Documentation:

- Administrative user guides
- Operational procedures manual
- Troubleshooting guides
- Training materials in required languages
- FAQ documentation

6.6 Maintenance Phase Deliverables

During the three-year maintenance period, the agency must provide:

Monthly Reports:

- System performance metrics
- Issue resolution status
- Enhancement implementations
- Security update status
- User support statistics

Quarterly Deliverables:

- System audit reports
- Performance optimization recommendations
- Security assessment updates
- Backup verification reports
- Enhanced feature documentation

6.7 Data Retention Phase

For the extended two-year data retention period, the agency must maintain:

- Data access mechanisms
- Reporting capabilities
- Security controls
- Audit logging
- Support documentation

6.8 Source Code and Intellectual Property

Upon project completion, the agency must transfer to NPC:

- Complete source code with documentation
- Development and deployment tools

SECTION 7 - FUNCTIONAL AND TECHNICALREQUIREMENTS

7.1 Infrastructure Requirements

The system requires a robust infrastructure foundation to support nationwide data collection and analysis operations. The agency must establish three distinct environments - development, testing, and production - each configured to meet specific operational needs. The production environment demands high-availability configuration in active-active mode to ensure uninterrupted service delivery.

Server infrastructure must be procured and hosted on MeitY empaneled Government Community Cloud (GCC) services. While the agency will manage this infrastructure throughout the contract period, ownership will vest with NPC. The infrastructure must support the following operational parameters:

Essential Infrastructure Specifications:

- Processor: Minimum frequency of 2.0 GHz
- Network: Subnet/network segment capability with firewall protection
- Storage: Scalable capacity for minimum 175,000 beneficiary records
- Backup: Weekly full system backup with 30-day retention
- Auto-scaling: Horizontal scaling capability without system downtime

7.2 Technology Stack

The agency must implement a modern, secure technology stack capable of supporting complex data collection and analysis requirements. The selected technologies should enable efficient development while ensuring long-term maintainability and security. The technology options listed below is indicative and not restricted to.

Approved Technology Options: For Backend Development:

- ASP.NET Core with Oracle/MS SQL
- PHP/Python with MySQL
- Node.js with MongoDB
- Java with PostgreSQL

For Frontend Development:

- Modern JavaScript frameworks (React/Angular/Vue)
- HTML5 and CSS3 with responsive design
- Progressive Web App capabilities
- Cross-browser compatible components

Input Control Requirements:

The system must integrate with enterprise-grade voice recognition and translation services supporting all required languages. These services must provide:

- Real-time voice-to-text conversion
- Neural machine translation capabilities
- Offline processing capabilities
- API-based integration

- Scalable processing capacity

7.3 Performance Requirements

The system must maintain consistent performance under varying load conditions. Response time requirements vary by operation type and user interface:

Dashboard Performance:

- Page load time: Maximum 2-3 seconds
- Report generation: Maximum 5 seconds
- Data visualization: Real-time updates
- Search operations: Under 2 seconds
- File downloads: Response within 3 seconds

Mobile Application Performance:

- Application launch: Under 3 seconds
- Form loading: Under 2 seconds
- Data synchronization: Maximum 5 minutes
- Offline operation: Seamless functionality
- Media upload: Optimized for varying network conditions

7.4 Data Management

The system must implement comprehensive data management capabilities ensuring data integrity, security, and accessibility throughout the five-year lifecycle. The data management framework should address both operational and retention requirements.

Data Handling Requirements: The system must efficiently process various data types including structured survey responses, GPS coordinates, photographs, and digital signatures. Data validation must occur at multiple levels to ensure accuracy and completeness.

Storage and Retention: During the three-year operational period, the system must maintain full data accessibility with real-time processing capabilities. The subsequent two-year retention period requires secure storage with continued access for reporting and audit purposes.

7.5 Security Implementation

Security measures must protect system components and data throughout the project lifecycle. The implementation must incorporate industry best practices and comply with government security guidelines.

Core Security Components:

- End-to-end encryption for data transmission
- Multi-factor authentication for user access
- Role-based access control implementation
- Comprehensive audit logging
- Regular security assessments

7.6 Integration Requirements

The system must support integration with existing systems and potential future additions. Integration mechanisms should follow standard protocols while maintaining security and performance requirements.

API Implementation: All APIs must implement:

- Secure authentication mechanisms
- Data validation controls
- Rate limiting
- Error handling
- Performance optimization

7.7 Compliance Requirements

The implementation must adhere to various compliance standards ensuring system reliability, security, and accessibility. Key compliance areas include GIGW guidelines, security standards, and accessibility requirements.

The agency must ensure:

- Regular compliance assessments
- Documentation of compliance measures
- Timely resolution of compliance issues
- Periodic compliance reporting
- Maintenance of compliance certificates

7.8 Support Requirements

The agency must provide comprehensive support throughout the contract period, including:

Operational Support: The onsite technical resource must provide first-level support during business hours. This individual should possess the expertise to handle routine maintenance, user support, and coordination with the offshore development team.

Technical Support: The agency must maintain a support system providing:

- Issue tracking and resolution
- Performance monitoring
- Security update management
- Feature enhancement implementation
- User training and documentation

Each requirement specified in this section serves as a minimum standard. The agency may propose enhanced capabilities where beneficial to system operation and user experience. All implementations must align with NPC’s objectives and Government guidelines for cyber security and Personal Data Protection Act while maintaining system security and performance standards.

SECTION 8 - REQUIRED DASHBOARD COMPONENTS & FEATURES

IN SCOPE BUT NOT LIMITED TO

8.1 Core Dashboard Components

Sl. No.	Component	Features
1.	**Administrative Dashboard**	- Multi-level administrative controls (Ministry, NPC, Zone, State, District) - User management and role assignment -System configuration management - Performance monitoring and analytics - Task assignment and tracking - Real-time system status monitoring
2.	**Survey Management**	- Questionnaire management in multiple languages - Survey assignment and tracking - Progress monitoring - Data validation rules management - Quality control metrics - Field investigator performance tracking
3.	**Data Analytics**	- Real-time data visualization - Custom report generation - Statistical analysis tools - Trend analysis - Geographic information system (GIS) integration - Multi-dimensional data analysis
4.	**Quality Control**	- Data validation dashboard - Error detection and reporting - Quality metrics visualization - Audit trail monitoring - Compliance tracking - Performance benchmarking

8.2 Administrative Interface

The dashboard must provide a comprehensive administrative interface supporting multi-level user management and system configuration. This interface serves as the primary control center for system operations, enabling administrators to manage users, monitor system performance, and configure operational parameters.

The administrative console must implement role-based access control, allowing different levels of administrative privileges based on user roles. Ministry-level administrators require complete system oversight, while state and district administrators need focused access to their respective jurisdictions. All user access and management capabilities need to be linked with provision of OTP based multi factor authentication on registered mobile numbers.

The interface must support the following administrative functions:

User Management Capabilities:

- Creation and management of user accounts across all administrative levels
- Role assignment and permission management
- User activity monitoring and reporting
- Access control modification
- User authentication management

8.3 Data Visualization

The dashboard must transform complex survey data into meaningful visual representations that aid decision-making. The visualization engine should support real-time data processing and display, offering various presentation formats suitable for different types of information.

Key Visualization Requirements:

- Interactive charts and graphs with drill-down capabilities
- Geographic information display through maps and heat maps
- Comparative analysis views across regions and time periods
- Statistical representation of survey responses
- Performance metric visualizations

8.4 Reporting Engine

The reporting system must provide both standard and customizable reporting capabilities. Users should be able to generate reports based on various parameters while ensuring data accuracy and consistency. The reporting engine must support:

Standard Reports: The system must provide pre-configured reports addressing common monitoring needs. These reports should cover operational metrics, survey progress, and implementation effectiveness across different administrative levels.

Custom Report Generation: Users must have the ability to create custom reports by:

- Selecting specific data parameters
- Choosing visualization formats
- Setting report periodicity

- Defining export formats
- Scheduling automated generation

8.5 Performance Monitoring

The dashboard must include comprehensive performance monitoring capabilities to track system health and operational efficiency. This monitoring system should provide real-time insights into:

System Performance Metrics:

- Server resource utilization
- Response time measurements
- User concurrency levels
- Database performance
- Application error rates

Operational Metrics:

- Survey completion rates
- Data synchronization status
- User activity levels
- Report generation statistics
- System availability measurements

8.6 Data Management Interface

The interface must provide tools for managing the extensive data collected through the survey process. This includes capabilities for:

Language Processing:The dashboard must support management of voice input and translation services including:

- Translation accuracy monitoring
- Voice recognition performance metrics
- Language model updates
- Translation dictionary management
- Input method analytics

Data Validation: The system should implement multi-level validation ensuring data quality through:

- Automated validation rules
- Manual verification workflows
- Error flagging and correction
- Data consistency checks
- Quality metric tracking

Data Export and Import: The system must support various data exchange formats while maintaining data integrity and security. Export capabilities should include options for:

- Multiple file formats (CSV, Excel, PDF)

- Selective data export
- Scheduled exports
- Secure data transfer
- Audit trail maintenance

8.7 Search and Analysis Tools

Users require powerful search and analysis capabilities to extract meaningful insights from collected data. The dashboard must provide:

Search Functionality:

- Advanced search filters
- Full-text search capabilities
- Parameter-based searching
- Results filtering
- Search history tracking

Analysis Tools: The system should offer analytical capabilities including:

- Trend analysis across time periods
- Regional performance comparisons
- Statistical analysis tools
- Pattern recognition
- Impact assessment metrics

8.8 Help and Support Features

The dashboard must incorporate comprehensive help and support features ensuring effective system utilization. These features should include:

Documentation Access:

- Context-sensitive help
- User guides and manuals
- Video tutorials
- FAQs and troubleshooting guides
- System update notifications

Support Interface: The system should provide mechanisms for:

- Issue reporting and tracking
- Feature request submission
- User feedback collection
- Knowledge base access
- Support ticket management

All dashboard components must maintain consistent performance while supporting concurrent access by 500 users. The interface should adapt to different screen sizes and resolutions while maintaining functionality and usability across various devices and browsers.

SECTION 9 -FEATURES OF SURVEY MOBILE APP BUT NOT LIMITED TO

9.1 Core Mobile App Features

Sl. No.	Component	Features
1.	User Interface	- Intuitive design for field investigators - Multi-language support (Hindi + English) - Customizable layout for various surveys - Support for both Android and iOS platforms - Offline-first design - Adaptive UI for different screen sizes
2.	Data Collection Tools	- Multiple input formats (text, multiple choice, ratings) - GPS location tagging - Media capture (photos, videos, audio) - Digital signature capture - Barcode/QR code scanning - Offline data storage and sync
3.	Training Module	- Interactive training content - Self-assessment tools - Progress tracking - Performance monitoring - Certification system - Offline learning support
4.	Field Operations	- Task management - Route optimization - Work status tracking - Real-time updates - Team communication - Emergency support

9.2 User Interface and Experience

The mobile application must provide an intuitive and efficient interface for field investigators conducting surveys across diverse geographic locations. Understanding that users will operate in varying conditions and may have different levels of technical proficiency, the interface must prioritize ease of use while ensuring data accuracy and completeness.

The application must support Hindi and English, with seamless language switching capabilities. Field investigators should be able to view questions, enter responses, and navigate the application in their preferred language. The interface must maintain consistent layout and functionality across all supported languages while accommodating different character sets and text directions.

Essential interface elements include:

- Clear question presentation with support for complex survey structures
- Intuitive navigation between survey sections
- Progress indicators showing completion status
- Error indicators highlighting validation issues
- Quick access to frequently used functions

9.3 Offline Functionality

The application must function effectively in areas with limited or no internet connectivity. This offline capability forms a crucial component of the system, ensuring uninterrupted survey operations across all geographic locations. When operating offline, the application must maintain all critical functionalities while ensuring data integrity.

Data Management in Offline Mode: The application must implement sophisticated data management, including:

- Local storage of survey responses with encryption
- Automatic synchronization when connectivity becomes available
- Progress tracking across online and offline modes
- Conflict resolution for data synchronization
- Storage optimization for extended offline operation

9.4 Data Collection Capabilities

The application must support comprehensive data collection through various input methods. Each input type requires specific validation rules and handling mechanisms to ensure data quality and consistency.

Survey Response Types: The application must handle multiple data formats including:

- Text entries with multi-language support
- Numeric inputs with validation rules
- Multiple choice selections
- Date and time inputs
- GPS coordinates
- Photographs and digital signatures
- Voice recordings when required

Voice Input and Translation Features:

The mobile application must implement sophisticated input controls for feedback questions. This includes voice-based text input capability, supporting all regional languages specified in the scope. The voice recognition system must maintain high accuracy across different accents and dialects within each supported language.

The application must provide automatic translation services, converting regional language inputs to English in real-time. This translation feature should:

- Maintain contextual accuracy

- Preserve technical terms without translation where appropriate

- Allow manual correction of translations if needed

- Store both original and translated text

- Maintain audit trail of translations

To ensure data integrity and prevent unauthorized data copying, the application must implement strict input controls including:

- Disabling copy-paste functionality in feedback input fields

- Preventing screenshot capture during feedback entry

- Blocking third-party keyboard applications

- Restricting sharing options during feedback entry

- Logging all input method changes

9.5 Location Services

Geographic information plays a vital role in survey validation and analysis. The application must implement robust location services while managing battery consumption and accuracy requirements. Location tracking should operate in both online and offline modes, with appropriate data storage and synchronization mechanisms.

Location features must include:

- Automatic GPS coordinate capture
- Location accuracy verification
- Geo-fencing capabilities
- Location history tracking
- Map-based navigation support

9.6 Quality Assurance

The application must implement multi-level data validation ensuring accuracy of collected information. These validations should operate in real-time, providing immediate feedback to field investigators while preventing submission of incomplete or incorrect data.

Validation Framework: The system implements hierarchical validation including:

- Field-level input validation
- Cross-field consistency checks
- Mandatory field verification
- Range and format validation
- Business rule compliance

9.7 Security Implementation

Given the sensitive nature of collected data, the application must implement comprehensive security measures protecting both stored and transmitted information. Security implementations must address device-level and network-level threats while ensuring user authentication and data integrity.

Security measures include robust authentication mechanisms, secure data storage, and encrypted transmission protocols. The application must maintain security standards even during offline operation, implementing appropriate controls for locally stored data.

9.8 Performance Optimization

The application must maintain responsive performance while managing large datasets and complex operations. Performance optimization should address device resource utilization, battery consumption, and storage management. Critical performance requirements include:

Response Times:

- Application launch: Under 3 seconds
- Form loading: Under 2 seconds
- Data save operations: Under 1 second
- Photo capture and storage: Under 3 seconds
- Synchronization initiation: Under 2 seconds

9.9 Integration Capabilities

The mobile application must maintain seamless integration with the central dashboard while operating independently when required. Integration mechanisms must ensure data consistency and synchronization accuracy across the system.

Synchronization Protocols: The application implements intelligent synchronization including:

- Selective data synchronization
- Background sync capabilities
- Bandwidth optimization
- Error recovery mechanisms
- Progress tracking and reporting

9.10 Support Features

The application must provide comprehensive support features ensuring effective operation in field conditions. These features should be accessible offline and provide immediate assistance to users encountering issues during survey operations.

Built-in support includes contextual help, troubleshooting guides, and offline documentation. Users should have access to simplified issue reporting mechanisms that function even in offline mode, with automatic submission when connectivity becomes available.

Each feature described must undergo rigorous testing under various operating conditions, ensuring reliable performance across different devices, network conditions, and usage patterns. The agency must provide regular updates and enhancements based on user feedback and operational requirements.

SECTION 10 -DELIVERABLES AND TIME FRAME

SECTION 10 - DELIVERABLES AND TIME FRAME

S.No.	DELIVERABLE	TIMEFRAME
1.	Signing of Contract Agreement & Submission of Performance Bank Guarantee	Within 7 days of issue of work order (T0)
2.	Inception Report, SRS, FRS and Design Documentation	Within 15 days of signing of contract agreement (T0+15)
3.	Development of Dashboard and Mobile Application& procurement of hosting server	Within 21 days of signing of contract agreement (T0+21)
4.	User Acceptance Testing & Deployment	Within 28 days of signing of contract agreement (T0+28)
5.	Maintenance and Support	For three years from the date of completion of deliverable at Sr. No. 4
6.	Data Retention and Management	Total 5 years (3 years operational period + 2 years additional retention)

Note: The development & Hosting process has to be completed within an overall timeline of twenty-eight (28) days. The agency must submit a detailed project plan encompassing all activities. While there may be variations in time limits for individual components, the overall timeline for completion of initial phases should not exceed twenty-eight (28) days. The project plan will be evaluated as part of the technical evaluation.

SECTION 11 - SCHEDULE OF PAYMENT

Sl. No.	Deliverable		Payment
1.	Inception Report (Outlining the survey methodology and timelines) and Design, Development, Installation, Testing of Survey Mobile App.		5% of the cost + GST as applicable will be payable along with work order for the study
2.	Design, Development, Installation, Testing of Dashboard and Mobile App on stage server.		20% of the cost + GST as applicable
3.	User Acceptance testing & Finalisation of the, Security Audit, Dashboard and Mobile App and Go Live & deployment on server its acceptance by Ministry.		20% of the cost + GST as applicable
4.	• Addressing day to day technical queries regarding IT system raised by the NPC and Ministry. • Minor developments in the deployed Mobile App and Dashboard to be incorporated at no extra cost. • Performance Optimization • Maintenance and updation of Dashboard and Mobile Application.	End of first year*	15% of the cost + GST
5.	• Addressing day to day technical queries regarding IT system raised by the NPC and Ministry. • Minor developments in the deployed Mobile App and Dashboard to be incorporated at no extra cost. • Performance Optimization • Maintenance and updation of Dashboard and Mobile Application.	End of Second Year*	15% of the cost + GST
6.	• Addressing day to day technical queries regarding IT system	End of Third year*	15% of the cost + GST

	raised by the NPC and Ministry. • Minor developments in the deployed Mobile App and Dashboard to be incorporated at no extra cost. • Performance Optimization • Maintenance and updation of Dashboard and Mobile Application.		
7.	Data Retention and retrieval	End of Fourth year*	5% of the cost + GST
8.	Data Retention and retrieval	End of Fifth year*	5% of the cost + GST

to be counted from the date of completion of deliverable at Sr. No. 3

SECTION 12 - PERFORMANCE BANK GUARANTEE

The selected agency is required to submit Performance Bank Guarantee, within 7 days from the issue of work order, for value equivalent to 5% of the contract value. The Performance Guarantee shall contain a claim period of 90 days from the last date of validity i.e., minimum period of 3 months from the date of completion of the work or date of expiry of contract whichever is later. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the delivery and warranty period.

SECTION 13: Confidentiality

a. The selected agency and their personnel will not, either during the term or after expiration of this contract, disclose any proprietary or confidential information relating to the services, contract or business or operations of NPC or its clients without the prior written consent of NPC.

b. The agency will ensure that no information about the software, hardware, database and the policies of the client organization is taken out in any form including electronic form or otherwise, from the client site by the manpower posted by them.

c. The agency or its deployed personnel, by virtue of working on NPC/Client's projects, can't claim any rights on the work performed by them. NPC/Client will have absolute rights on the work assigned and performed by them. Neither any claims of the agency or its deployed professionals will be entertained on the deliverables.

SECTION 14: INDEMNITY

a. The selected agency will indemnify NPC of all legal obligations of its professionals deployed for NPC projects.

b. NPC stand absolved of any liability on account of death or injury sustained by the Agency staff during the performance of this Bid and also for any damages or compensation due to any dispute between the agency and its staff.

SECTION 15 – GENERAL TERMS & CONDITIONS

The selected agency will not, without NPC's prior written consent, disclose theContract, or any provision thereof, or any specification, plan, sample of information furnished by or on behalf of NPC in connection therewith, to any person other than a person employed by the agency in the Performance of the Contract. Disclosure to any such employed person will be made in confidence and will extend only so far as may be necessary for purposes of such performance.

a. The selected agency will not outsource the work to any other associate/franchisee/third party under any circumstances. If it so happens then NPC will impose sanctions which will include: forfeiture of the security deposit, revocation of bank guarantees (including the ones submitted for other work orders) and termination of the Contract for default.

b. NPC may by written notice sent to the selected agency, terminate the work order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination will specify that termination is for NPC's convenience, the extent to which performance of work under the work order and /or the contract is terminated, and the date upon which such termination becomes effective. NPC reserves the right to cancel the remaining part and pay to the selected agency an agreed amount for partially completed Services.

c. In the event of the agency's company or the concerned division of the company is taken over / bought over by another company, all the obligations under the agreement withNPC, should be passed on for compliance by the new company / new division in the negotiation for their transfer.

d. All panel agencies automatically agree with NPC for honouring all aspects of fair trade practices in executing the work orders placed by NPC.

e. The Technical support to the project will be provided throughout the country and the period for which the support is required will be indicated by NPC from time to time.

f. Dashboard and Survey Mobile App should be in Mobile/Tablet Responsive, so it adapts and fit design as per user resolution.

g. Dashboard should be Compatible to all latest browsers (i.e., Firefox, Microsoft Edge, Internet Explorer, Opera, Mozilla, Google Chrome, Safari etc.)

h. Agency would acquire the security certificate to certify the Dashboard and Mobile app as secured. Security Audit for the dashboard hosted on server. Agency needs will have to resolve any security concern raised by the IT security Auditor. Agency has to provide information related to support and remediation process.

i. The cost of security audit shall be borne by the Agency. The Agency shall be responsible for removing all the bugs reported during the security audit to ensure that all vulnerabilities are fixed, and for getting the security audit cleared.

j. The Agency shall provide the support & maintenance on fixing the bugs, minor changes, data collection, data validation, data conversion, integration of the data for the application & monitoring the Dashboard services & survey mobile app, for three years from the date of completion of Dashboard and Survey Mobile App.

k. Dashboard must contain separate interface for Uploading of survey data with a function/facility of storing, visualization, updating & addition of database.

l. Features in Survey Mobile App and Dashboard shall not be limited to existing application. Detailed features/requirements shall be finalized during the requirement gathering phase.

m. The Dashboard need to be deployed on the Server. It should be designed & developed in a way to let the IPR rights remain vested with NPC. Dashboard & Mobile App needs to be developed using open-source technologies to avoid any product or periodic license fees etc. NPC shall be the sole owner of all IPR for the Dashboard and Survey Mobile App.

n. Latest technology must be used which is compatible with Government of India guideline.

SECTION 16– PENALTY CLAUSE:

1) National Productivity Council (NPC) reserves the right to deduct the penalty either from Performance Bank Guarantee or from pending bills submitted for the work already performed by the agency.

2) The liquidated damages for delay by Bidder shall be applicable under following circumstances:

   a. If the deliverables are not submitted as per schedule, the Agency shall be liable to pay 1% (One Percent) of the proportional cost of the services applicable at that stage of deliverables (Schedule of Payment) for delay of each week. or part thereof subject to Sl. No. 3 below of this penalty clause.
   b. If the deliverables are not acceptable to National Productivity Council as mentioned in Sl. No 2, Para (d) of this penalty clause, and defects are not rectified to the satisfaction of National Productivity Council within 30 (Thirty) days of the receipt of the notice, the Agency shall be liable for Liquidated Damages for an amount equal to 1% (One percent) of the amount admissible related to that stage of deliverables (as per Schedule of payment) for every week or part thereof for the delay in rectifying the deficiencies subject to Sl. No. 3 of this Penalty clause.
   c. Notwithstanding, anything mentioned above, the Agency shall not be made liable for any delay due to non-availability of timely approval and timely review by National Productivity Council/ Ministry or its state level counterparts or any stake holders not directly attributable to the Agency.
   d. If the deliverables submitted by the Bidder are not acceptable to National Productivity Council, reasons for such non-acceptance should be recorded in writing; National Productivity Council shall not release the payment due to the Agency. This is without prejudice National Productivity Council's right to levy any liquidated damages under Penalty clause. In such case, the payment will be released to the Agency only after it resubmits the deliverable and which is accepted by National Productivity Council.
   e. The Agency has to ensure the Dashboard and Mobile Application & features are available for use for at least 98% of the working time in a month. If the downtime increases beyond 2% of total working time in a month, penalty as per the table given below may be levied.

S. No	**Downtime % in a month as % of total working time**	**Penalty for each month**
1	<2%	No penalty
2	>=2% and <3%	0.5% of the total value of the contract
3	>=3% and <4%	1% of the total value of the contract
4	>=4% and <5%	2 % of the total value of the contract
5	>5%	National Productivity Council shall initiate termination of the contract

A logbook shall be maintained for keeping the records of each occurrence of downtime and entry shall be made in the logbook after mutual agreement.

3) The amount of liquidated damages for delay by Agency under this Contract shall not exceed 5 % (Five Percent) of the total value of the Contract as specified in the contract agreement.
4) If the services of the Agency are found unsatisfactory and objectives of the study/survey are not fulfilled in spite of giving adequate opportunity to the Agency, National Productivity Council may forfeit the amount due in part or whole, in addition to performance guarantee.

5) Agency has to timely inform about network security firewalls to be installed so that no data/information is lost due to malwares or other system viruses. If some kind of data/information loss happens due to technical glitches, then penalty up to 5% of the contract value may be levied subject to Sl. No. 3 of this penalty clause.

SECTION 17 - TERMINATION FOR INSOLVENCY & DEFAULT

The contract between NPC and the selected agency may be terminated under various circumstances, each requiring specific procedures to ensure orderly transition and protection of interests for all parties involved. This section outlines the conditions, procedures, and obligations related to contract termination.

17.1 Termination for Insolvency

In the event the agency becomes bankrupt or otherwise insolvent, NPC maintains the right to terminate the contract by providing written notice of four weeks. This termination will occur without compensation to the agency, ensuring protection of public interests and resources. During the notice period, the agency must maintain all system operations and facilitate an orderly transition of services.

The agency must sustain system availability and performance throughout the notice period while preparing comprehensive documentation of current system status, operational procedures, and technical configurations. This documentation becomes crucial for ensuring service continuity through the transition period.

17.2 Termination for Default

Contract termination may occur when the agency fails to meet its contractual obligations. Default conditions encompass failure to deliver services within specified timelines, inability to maintain performance standards, security breaches, non-compliance with statutory obligations, or unauthorized system modifications.

Upon identifying a default condition, NPC will issue a formal notice to the agency. The agency receives 30 days to implement corrective measures addressing the identified issues. Failure to adequately resolve these issues within the stipulated period empowers NPC to proceed with contract termination.

17.3 Termination for Change in Requirements

NPC reserves the right to terminate the contract when the underlying work requirement ceases to exist or undergoes substantial changes. This provision acknowledges that government policies, program requirements, or operational needs may evolve, potentially making the current system implementation unnecessary or requiring fundamentally different approaches.

In such cases, NPC will provide 90 days' written notice to the agency. This notice period allows for proper system documentation, data preservation, and orderly transition of services. Unlike termination for default, this scenario entitles the agency to fair compensation for services rendered and reasonable costs associated with early termination.

17.4 Voluntary Termination by Agency

The agency may request contract termination by providing 180 days' written notice to NPC. Valid grounds for such requests include force majeure conditions exceeding 60 days, payment defaults by NPC exceeding 90 days, material breach of contract by NPC, or unforeseen technical complications that fundamentally impact service delivery.

The extended notice period ensures adequate time for NPC to arrange alternative service provision while maintaining system continuity. The agency must continue providing all contracted services throughout the notice period while preparing for systematic knowledge transfer.

17.5 Transition Requirements

Regardless of termination type, the agency bears responsibility for ensuring smooth transition of services. The transition period focuses on maintaining system continuity while transferring knowledge and assets to NPC or its designated new service provider.

During transition, the agency must provide comprehensive system documentation including current configurations, operational procedures, security implementations, and maintenance requirements. Knowledge transfer sessions must cover technical aspects, system administration, troubleshooting procedures, and security protocols.

17.6 Financial Settlement

Financial settlement procedures vary based on termination type:

For termination due to changes in work requirements, the agency receives compensation for:

- Services delivered until the termination date
- Reasonable demobilization costs
- Transition support expenses
- Resource reallocation costs
- Documentation and knowledge transfer efforts

In default scenarios, NPC will compensate for services rendered up to the termination date, less applicable penalties and damages. The agency must provide detailed service delivery documentation supporting their payment claims.

17.7 Data and Asset Management

Throughout any termination process, the agency must ensure:

- Complete preservation of all system data
- Secure transfer of all intellectual property
- Return of any NPC-provided assets
- Proper disposal of sensitive information
- Documentation of all data handling procedures

17.8 Post-Termination Obligations

Both parties maintain ongoing obligations following contract termination. The agency must continue protecting confidential information and intellectual property rights while providing emergency support during the transition if required. NPC must fulfill all legitimate payment obligations and provide necessary access and support during the transition period.

17.9 Communication and Documentation

All termination-related communications must follow formal channels with proper documentation. This includes:

- Written notices with clear justification
- Formal acknowledgments of receipt
- Documented transition plans
- Progress reports during transition
- Final handover documentation

This comprehensive framework for contract termination ensures protection of both parties' interests while maintaining system continuity and data security throughout the transition process. All termination activities must prioritize public interest, data protection, and service continuity.

SECTION 18 - FORCE MAJEURE

a. Force majeure clause will mean and be limited to the following in the execution of the contract / purchase orders placed by NPC:-

- War / hostilities.
- Riot or Civil commotion.
- Earthquake, flood, tempest, lightning or other natural physical disaster.
- Restriction imposed by the Government or other statutory bodies, which is beyond the control of the agencies, which prevent or delay the execution of the order by the agency.

b. The agency will advise NPC in writing, duly certified by the local Chamber of Commerce, the beginning and the end of the above causes of delay, within seven days of the occurrence and cessation of the force majeure conditions. In the event of a delay lasting for more than one month, if arising out of clauses of force majeure, NPC reserve the right to cancel the order without any obligation to compensate the agency in any manner for what so ever reason.

SECTION 19: ARBITRATION

NPC and the agency/vendor will make every effort to resolve amicably, by direct negotiation, any disagreement or dispute arising between them under or in connection with the work order. If any dispute will arise between parties on aspects not covered by this agreement, or the construction or operation thereof, or the rights, duties or liabilities under these except as to any matters the decision of which is specially provided for by the general or the special conditions, such dispute will be referred to two arbitrators, one to be appointed by each party and the third to be appointed by the Director General, National Productivity Council, New Delhi and the award of the arbitration , as the case may be, will be final and binding on both the parties. The arbitrators or the umpire as the case may be, with the consent of parties, may modify the time frame for making and publishing the award. Such arbitration will be governed in all respects by the provision of the Indian Arbitration Act, 1996 or later and the rules there under and any statutory modification or re-enactment, thereof. The arbitration proceedings will be held in New Delhi, India.

APPLICABLE LAW

The work order will be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing.

SECTION 20: EARNEST MONEY DEPOSIT:

20.1 All bids must be accompanied by a bid security (EMD) for an amount of **Rs. 1,00,000/-** and any bid not accompanied by the required bid security (EMD) would not be opened. EMD can be provided in the form of banker’s cheque/ Bank transfer (NEFT, RTGS transaction)/ demand draft. Demand draft or banker's cheque to be issued in favour of ‘National Productivity Council’. Scanned copies of banker’s cheque/ Bank statement (in case of NEFT, RTGS transaction)/ demand draft/ of EMD need to be uploaded while submitting bids.

20.2 Original copy of banker’s cheque or demand draft should reach at Group Head (IE), National Productivity Council, Utpadakata Bhawan, Lodhi Road, New Delhi – 110003 before the due date & time of opening of technical bid.

20.3 The Bidder should submit the Bid Security Declaration Form-6 and Earnest Money Deposit (EMD) as mentioned in above the bid document.

22.4 Any bid not accompanied by the EMD would be rejected by NPC as being non-responsive.

22.5 EMD of unsuccessful bidder would be return after the acceptance of Letter of award by the successful bidder and EMD of successful bidder will be return on submission of Contract Performance Guarantee.

22.6 No Interest will be payable by National Productivity Council on the EMD.

22.7 Relaxations if applicable for MSME for submission of EMD would be as per Government orders.

22.8 For NEFT/RTGS, bank details of NPC are as under:

Name of Organization; **National Productivity Council**
Bank: Indian Overseas Bank; Branch: Golf Links, New Delhi
A/C No.: 026501000009207; IFSC: IOBA0000265; MICR code: 110020007

SECTION 21 – ELIGIBILITY CRITERIA

a. The Agency should be a Company registered in India under the Companies Act 1956 or a partnership registered under the India Partnership Act 1932 and/or startup and/or the entities incubated at government recognized universities/academic institutions such as IIMs/IITs/NITs/Central and Government Universities and/or a Society constituted under a Ministry /Department of the Government of India and registered under the Societies Registration Act 1860 or a limited liability partnership firm and/or Not for Profit organization operating in India for not less than 3 years.

b. The agency should be operating in the field of Software development and software solutions.The agency must have 5 years' experience in executing similar kind of projects.

c. The agency with an minimum annual turnover/ revenue of Rs. 3 croresfrom software development engagement consecutively for the past three years. A copy of the Balance Sheet/an authentic document, clearly specifying software development turnover/revenue, of the company for the year **2021-22, 2022-23 & 2023-24**. may be enclosed as proof for the turnover/revenue

d. The agencies must have themselves developed and implemented **minimum 2 Dashboard and 2 Survey Mobile App development projects** for the government sector (in India) in the last three years viz. **2021-22, 2022-23 & 2023-24**. For the total IT projects, the software development component should be unambiguously verifiable from the purchase orders otherwise the project will not be considered. Similarly, projects falling outside mentioned period will not be considered. Copies of Purchase orders and linked satisfactory completion certificates from the clients should be submitted as supporting documents and Information, on the projects, may be furnished as per **Form 3.**

e. The agency must demonstrate experience in implementing voice recognition systems, developing multi-language translation features and creating secure input control mechanisms.

f. The agency should hold a valid ISO 9001 certification for working in the area of software development.

g. The agency should hold a valid ISO 27001 certification for working in the area of software development.

h. The agency should hold a valid ISO 20000 certification for working in the area of software development.

i. In case of Bid, Agency would deploy resources, working on its rolls, as per NPC project requirements from time to time.

j. The selected agency would sign a non-disclosure agreement in addition to an undertaking that the software developed by their professionals for NPC projects wouldn't be used by them for any other purpose.

k. The Copyright of the developed software/application would remain with the NPC and/or the respective user organization (client) as the case may be.

l. The service has to be provided anywhere in India.

m. The firm/companies will only participate in the solutions which fulfil all the Eligibility Criteria as mentioned in this BID document.

n. The agency should be registered with the Goods and Service Tax department and carry a valid PAN, GST.

o. The agency should provideMemorandum of Articles of Association (in case of registered Agency(s)), Bye laws and certificates for registration (in case of registered co-operative societies), Partnership deed (in case of partnership firm). Only the relevant pages highlighting the '**Object Clause**' and not the whole document need besubmitted.

p. A self-attestedcertificate that the company has not been blacklisted by an authorized agency of the State/Central Government and there have been no litigations with any State/Central Agency over the execution of IT projects.

In order fortheBIDs to be considered, the Agencies are requested to submit documents for each of the above clauses.

SECTION 22 - BID SUBMISSION PROCESS

Submission of BID

a. The bid would consist of two parts "Technical Proposal" and "Financial Proposal" and should be duly submitted online using the e-Procurement Portal GeM on or before the due date and time. The Technical Proposal should contain Form-1, Form 2(A), Form 2(B), Form 2(C), Form -3, Formats-4 and Form 6 &Financial proposal should contain Form-5 as described below. All the forms should be duly filled and signed by authorized signatory. In case the bidder fails to submit any of the formats, the bid would be considered as unresponsive.

b. Agencies are advised to study the BID Document carefully. Submission of the BID will be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and requirement specifications in the BID document with full understanding of its implications. BIDs not complying with all the given clauses in this BID document are liable to be rejected. Failure to furnish all information required in the BID Document or submission of anBID not substantially responsive to the BID document in all respects will be at the agency's risk and may result in the rejection of the BID.

c. All pages of the BID being submitted must be signed and sequentially numbered by the Agency(s) irrespective of the nature of content of the documents. Un-signed & un-stamped bid shall not be accepted.

Selection Methodology

The selection/ evaluation committee of NPC shall rate the agencies based on "pre-defined parameters". These parameters have been formed on the basis of above scope of work and mentioned in **evaluation Criteria of the RFP.**

Opening of Technical Proposal

The Technical Proposal will be opened **online**in the presence of the authorized representatives of the bidders, who wish to be present.

The agencies are required to make technical presentation before the Technical Evaluation Committee constituted by the competent authority of NPC for which with prior intimation would be sent to the qualified/ shortlisted agency.

The price Bids of only those agencies (agency) would be opened which are technically qualified with more than or equal to **50 out of 100** marks in the technical presentation based on pre-defined parameters.

If there is more than one technically qualified agency, the agency which **scoremaximum marks in QCBS {70% weightage to Technical Score (T): 30% weightage to Financial Score(F)}** would be considered for award of job.

In the unlikely event of a tie in the total score between two or more agencies, the technical bid of the agency which secured the highest number of points in the technical round will be considered for award of the job/ work.

Award of Work

The work would be awarded to a qualified Vendor with expertise in Dashboard/website development and Mobile App, who would act as the Sr. Solution Architect for this project. The Sr. Solution Architect (SSA) would cater to all requirements of Portal & Mobile Application pertaining to design, development, maintenance, and other requirements as defined under this document.

The Portal would be hosted with any of the MeitY empaneled Government Community Cloud (GCC) Service Providers.

Development should be compliant to audit requirements issued by GOI.

During the implementation phase i.e. before go live any change in laws/ regulations should be catered by the Dashboard/Portal and Mobile App.

SECTION 23 - UPLOADING OF BIDS

a. BIDs, complete in all respects, must be submitted by the due date and time as per the submission process given in this BID document. In the event of the specified date for the submission of BID is a declared holiday, the BIDs can be uploaded up to the given time on the next working day for which NPC will make necessary provisions.

b. NPC may, at its own discretion, extend the date for uploading of BIDs. In such a case all rights and obligations of NPC and the Agencies will be applicable to the extended time frame.

c. NPC will not be responsible for any delay on the part of agencies in downloading the BID document or submission of BID documents before the due date and time of submission.

d. The BID submitted by telex/fax/Email or any manner other than specified above will not be considered. No correspondence will be entertained on this matter.

e. At any time prior to the last date for receipt of BIDs, NPC, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective agency, modify the BID Document by an amendment. The amendment will be notified onGeM and CPPP portaland should be takeninto consideration by the prospective agencies whilepreparing their BIDs.

f. In order to give prospective agencies reasonable time to take the amendment into account in preparing their BIDs, NPC may, at its discretion, extend the last date for the receipt of BIDs. No BID may be modified subsequent to the last date for receipt of BIDs. No BID may be withdrawn in the interval between the last date for receipt of BIDs and the expiry of theBID validity period specified by the agency in the BID.

g. The agencies will bear all costs associated with the preparation and submission of their BIDs. NPC will, in no case, be responsible or liable for those costs, regardless of the outcome of the BID submission process.

h. In case terms and conditions of the BID document are not acceptable to any agency, they should clearly specify the deviations in their BIDs.

The BIDs will then be passed on to a duly constituted Technical Evaluation Committee (TEC).

SECTION 24 - EVALUATION OF BID

a. When deemed necessary, NPC may seek clarifications on any aspect of the BID from the agency. However, that would not entitle the agency to change or cause any change in the substance of the BID submitted. This would also not mean that their BID has been accepted.

c. Any effort by an agency to influence NPC's BID evaluation, BID comparison or contract award decisions may result in the rejection of the agency's BID.

d. NPC reserves the right to accept any BID, and to cancel/abort the BID process and reject all BIDs at any time prior to award of Contract, without thereby incurring any liability to the affected agencies or agencies and of any obligation to inform the affected agencies of the grounds for NPC's action and without assigning any reasons.

e. NPC also reserves the right to float a fresh BID any time during the currency of Bid of this BID without assigning any reason.

TECHNICAL EVALUATION

The agencies as per the BID specifications. BIDs, not satisfying the eligibility criteria will be rejected. However, the TEC reserves the right to call for additional information from the agencies to fully establish their eligibility.

TheBid criteria shall be based on the following:-

AGENCY PROFILE

- **Financial Strength** (Minimum Annual Turnover/ revenue of Rs. 3 Cr from software development engagement in each of the previous three financial years)
- **Human Resource Competence** (Minimum20 Full Time Application development professional on their own payroll as on date of submission)
- **Technical Competence** (Valid ISO 9001, ISO 27001and ISO 20000certification and preferably dedicated operational software development centre within Delhi NCR along with certified and audited own Data Centre of the agency)

NPC will evaluate the agencies for short listing, based on weightages assigned to each of the Bid criteria.

The NPC will short list the agency, who secure the 50 Marks [i.e. minimum required marks].

a. Subsequently, the NPC would examine the technical details and may ask for additional information and may call the eligible agencies for a presentation of the projects handled by them and quoted in their BIDs.
b. The time limit, in which the agencies' have to submit the additional information or present their projects, will be decided by the NPC and its decision will be final in this regard.
c. The agencies will also assist the NPC in getting relevant information from the agencies' references.
d. Agencies failing to adhere to the specified time limit will not be considered for further evaluation.

SECTION 25: EVALUATION CRITERIA

S No	Criteria	Scoring matrix	Maximum Marks	Remarks
1.	Average annual turnover/ revenue in INR from assessment services only for last 3 financial years	• Equal to or greater than Rs 10Crore: **15 marks** • Equal to or greater than Rs 7 Crore & Less than Rs 10 Crore: **10 Marks** • Equal to or greater than Rs **5 Crore**& Less than Rs 7Crore: **7 marks** • Less Than 5 Crore:**3 marks**	15	Form 2(A) and Audited financials to be enclosed.
2.	Experience in Design & Development of Dashboard and Mobile App for any Govt. Dept. in last three years of work order value. (The project should be related to only software. No Hardware and software license related work will be considered as a part of the scope. Maximum 3 work orders are allowed in total.)	• Equal to or greater than Rs 90 Lacs: **15 marks** • Equal to or greater than Rs 70 Lacs& Less than Rs 90 Lacs: **10 Marks** • Equal to or greater than Rs **50 Lacs** & Less than Rs 70 Lacs: **5 marks**	15	FORM- 3 + Work Order Copy + STQC Certificate + Security Audit Certificates
3.	Experience in development of Dashboard and Mobile Appand experience of getting the Dashboard and Mobile App Audited from CERT-IN Empaneled vendors. (Govt. Dept.)	• 11 to 14 Dashboard and Mobile app or More: 15 Marks • 8 to 10 Dashboard and Mobile app: 10 Marks • 4 to 7 Dashboard and Mobile app: 5 Marks	15	FORM- 3 and STQC Certificate + Security Audit Certificates
4.	Number of regular/On roll Employees involved in software application development	• 50 and above Employees: 10 marks • Equal to or greater than 40 to & less than 50 Employees: 7 marks • Equal to or greater than 20 to & Less than 40 Employees: 5 marks • Less than 20 Employees: No marks	10	FORM- 2 (B) and documentary evidence to be provided.

5.	Valid ISO 20000, ISO 27001, ISO 9001 Certificate (Validity of the certificates should be for the period of one year since the date of submission of EOI)	• ISO 27001, ISO 20000 and ISO 9001: **5 marks** • ISO 27001 & ISO 20000: **3 marks** • Only ISO 20000 **OR** ISO 27001: **2 marks** • Only ISO 9001 **OR** No certification: **No marks**	5	FORM- 2 (C) and documentary evidence to be provided
6.	Agency/Firm has an operational dedicated software development centre within Delhi NCR	• If an operational dedicated software development centre within Delhi NCR – 5 Marks • If does not have operational dedicated software development centre within Delhi NCR - No marks	5	FORM- 2 (C) and documentary evidence to be provided
7.	Agency/Firm with owned & secured data centre in India	• If owned, secured & in India: 10 Marks • If hired, secured & in India: 5 marks • If No: No marks	10	FORM- 2 (C) and documentary evidence to be provided
8.	Understanding of the Project Approach, Methodology,Team Composition and Timelines.	To be submitted in Technical Proposal	10	FORM- 4
9.	• Company profile • Understanding of project and Proposed Solution • Innovative Ideas and Suggestion	Technical Presentation	15	

SECTION 26 - STANDARD FORMS

FORM-1: BID SUBMISSION FORM
(To be submitted on the letter head of the Agency(s))

To

Director & Group Head (IE)
National Productivity Council
Lodi Road, New Delhi 110003

Subject: Submission of the Bid with NPC forproviding Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three years

Dear Sir,

We, the undersigned, offer to provide Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three yearsto NPC that are implementing the projects in accordance with your Biddocument dated __________. We are hereby submitting our BID for providing Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three years

We hereby declare that all the information and statements made in this BID Document are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of the BID document. We understand you are not bound to accept any proposal you receive.

Yours sincerely,

Authorized Signature [*In full and initials*]: __________________________

Name and Title of Signatory: ___________________________________

Name of Firm: ____

Address: ____

Location: _____________________________________Date: __________

FORM- 2 (A): AGENCY PROFILE - FINANCIAL COMPETENCE

a) Name of the Agency: ______________________________

b) Incorporated as _______________ in year ____________________ at ____________

(State Registered Firm, Co-operative Society or Partnership Firm)

c) Agency profile (*)

Agency Registered Address:______

E-mail: _______________

GSTNo:__________

PAN: _______________

Name of the top executive with designation: _______________

Telephone No:_____________

Mobile: _______________

Email: _______________

d) Average annual turnover/ revenue of the agency in INR from assessment services only for last three financial years __________, ____________, _________________.)

FinancialYear	Total Turnover/ revenue (netoftaxesandduties) from software development projects/activities Turnover/ revenue Figures': (In Rs. Crores)
FY:	
FY:	
FY:	

Average Turnover/ revenue during Last 3 (three) Years…………

Authorized Signature [*In full and initials*]: __________________________

Name and Title of Signatory: ____________________________________

Name of Firm: ____

Address: ____

Location: ______________________________________Date: __________

Note:*Consolidated Audited Annual Reports/Financial Statements for last three financial years have to be provided as proof for firm's turnover/revenue.*

FORM- 2 (B): AGENCY PROFILE - HUMAN RESOURCE COMPETENCE

Details of Educational Qualifications & Experience of Technical Professionals on permanent rolls of company.

a) Number of regular Employees involved in software application development

Technical Manpower Strength: Technical Professionals: _____ Nos.

Sl No	Resource Category	Prescribed Qualifications	Minimum Prescribed experience	Number of full-time resource persons (for each resource category) till date
-1	-2	-3	-4	-5
1	Sr Solution Architect	BE/B Tech /MCA with specialization in computers	15 years (with Relevant Experience)	
2	SolutionArchitect	Do	10 years (Ability to assess project needs in various domains)	
3	Project Manager	Do	10 years (In managing large Software development projects)	
4	Softwaredesigner	Do	5 years (in software designing for large software development projects)	
5	Tech lead/ Sr Developer	Do	3 years (In software development projects)	
6	Developer	Do	1 year (In software development projects)	
			Total	

Name and Title of Authorized Signature: ________________________________

Name of Firm: ____

Address: ____

Location: ____________________________________Date: ______________

***Note**: - Refer **Annexure – I** for Educational Qualifications & Experience of Technical Professionals details.*

ANNEXURE- I: EDUCATIONAL QUALIFICATIONS & EXPERIENCE OF TECHNICAL PROFESSIONALS ON PERMANENT ROLLS OF COMPANY.

All degrees/diplomas should be in first class pursued through a full-time course of a government recognized university/institution

1. **Developer**

   MCA / BE / B. Tech with specialization in computers with 1+ years' experience on Software Development Projects

2. **Tech-lead/Sr. Developer**

   MCA / BE / B. Tech with specialization in computers with 3+ years' experience on Software Development Projects and capable of leading a team of developers.

3. **Software Designer**

   MCA / BE / B. Tech with specialization in computers with 5+ years' experience in software designing for major software development projects. The incumbents should be well informed of the latest technology development in hardware and software tools.

4. **Project Manager**

   MCA / BE / B. Tech with specialization in computers or equivalent with 10+ years' experience of managing large software development projects. The incumbents must have independently handled at least two large projects on all aspects from concept stage to implementation. They should be strong in the assessment of project needs and their resolutions, system integration, quality assurance besides handling project teams. They should be aware of technology tools and deployment issues.

5. **Solution Architect**

   MCA / BE / B. Tech with specialization in computers or equivalent with 10+ years' experience of assessing project needs in various domains. The incumbent must be able to offer value addition to the projected requirements with respect to future needs and socio-economic aspects. Selection and application of technology must be their strength and must be capable of managing multiple projects.

6. **Sr. Solution Architect**

   The incumbent with relevant experience of 15+ years should be able to steer a project ab-initio. Person should have strength in technology, domain, and application development and possess leadership qualities to lead a team of 40-50 professionals.

***Note:** The professionals to be deployed on NPC projects have to be the regular employees of the selected agency. Therefore, the agency, who can't spare their working professionals for deployment on NPC projects, for durations exceeding one year, need not participate in this BID.*

FORM- 2 (C): AGENCY PROFILE - TECHNICAL COMPETENCE

a) Agency has validISO 9001,ISO 27001 and/or ISO 20000 Certificate and the validity of the certificates is for the period of one year since the date of submission of this BID. (Kindly enclose the self-attested copies of the same)

b) If the Agency/Firm has an operational dedicated software development centre within Delhi NCR: Yes/No

If yes, please provide details of the software development centre as per item (e) above.

Agency Address:

E-mail:

GST No:

PAN:

Name of the top executive with designation:

Telephone No: Mobile:

Email:

c) If the Agency/Firm has its owned & secured data centre in India: Yes/No

If yes, please provide details

d) Whether any Legal Arbitration/proceeding is instituted against the Agency or any of its directors have been convicted by any court of law or blacklisted by either any Government concern or any criminal case be pending against such concern by any government: Yes/No

Authorized Signature [In full and Initials]: ______________________________

Name and Title of Signatory: ____

Name of Firm: ____

Address: ____

Location: ____________________________________Date: ______________

Note: *Documents in support of the above may be furnished with page numbers indicated in the index. Please use separate sheets wherever necessary.*

FORM- 3: RELEVENT EXPERIENCE - PROFESSIONAL/PRACTICAL COMPETENCE

a) Please specify **Dashboard and Mobile App** development projectscompleted during __________, ____________, _________________.(last three years) Information may be submitted in the following format. Please attach separate sheet for each project and submit unambiguous work orders & satisfactory completion certificates from the clients.

S.No.	**Description**	**Government/ Private**	**Details of Dashboard**	**Details of Mobile App.**
1.	Name of the Client with phone number and address			
2.	Activities/Summary relevant to Scope			
3.	Project Duration			
4.	Work Order No. & Date			
5.	Month and Year of Work Completion			
6.	Work Order Value			
7.	STQC Certificate			
8.	Security Audit Certificates			

Note: Attach LOI/Work Order/ Contract copy/ Satisfactory Work Completion Certificates from Clients (Mandatory)

Authorized Signature [In full and Initials]: ________________________________

Name and Title of Signatory: ____

Name of Firm: ____

Address:____

Location: _______________________________________Date: ________________

***Note:**Supporting documents (Work order and Completion certificate, Client certificate to be enclosed) in support of the above may be furnished with page numbers indicated in the index. Please use separate sheets wherever necessary.*

FORMATS- 4: UNDERSTANDING OF THE PROJECT APPROACH, METHODOLOGY, TEAM COMPOSITION AND TIMELINES

(Formats for Project Approach, Methodology, Team Composition and Timelines)

4.1 Project Approach

Project Title:
[Insert Project Title]

Objective:

Scope of Work:

- **Deliverables**:
- **Key Features**:
- **Out-of-scope Items**:

Approach:

Project Phases:

1. **Initiation**:
2. **Planning**:
3. **Execution**:
4. **Monitoring & Control**:
5. **Closing**:
6. **Maintenance for 3 years**

Risk Management:

- **Potential Risks**:
- **Mitigation Plans**:

4.2 Methodology

Methodology Overview:

Detailed Methodology:

- **Phase 1: Requirement Gathering & Design**

  - **Activities**:
  - **Deliverables**:

- **Phase 2: Development (Dashboard + Mobile App)**
  - **Activities**:
  - **Deliverables**:
  - Duration:

- **Phase 3: Quality Assurance & Testing**
  - **Activities**:
  - **Deliverables**:
  - **Duration**:

- **Phase 4: Deployment & Feedback Loop**
  - **Activities**:
  - **Deliverables**:
  - **Duration**:

- **Agile/Scrum DetailsSprints**:
  - [Number of Sprints, e.g., 6 Sprints]
  - **Sprint Duration**:
  - **Sprint Goals**:

Collaboration Tools:

- **Communication**
- **Project Tracking**:
- **Version Control**:

4.3 Team Composition

Team Structure Overview:

Role	Team Member	Responsibilities	Experience
	[Name]	- Oversee overall project execution.	

4.4 Timelines

Timeline Overview:

Phase	Start Date	End Date	Key Milestones/Deliverables
Phase 1:			
Phase 2:			
Phase 3:			
Phase 4:			
Phase 5:			

Milestone-Based Timeline:

Phases	Date	Status

- [Briefly describe how potential risks will be identified, mitigated, and managed throughout the project.]

FORM- 5: FORMAT FOR FINANCIAL BID SUBMISSION

Subject:**Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three years**.

Dear Sir,

I/We, the undersigned having examined the above referred RFQ and hereby offer to submit our bid to undertake the subject assignment with total bid value and break-up furnished below.

Sr. No.	**Project Cost Head**	**Cost (A) (Rs.)**	**GST (B) (Rs.)**	**Amount (C) =(A+B) (Rs.)**
1	Design, Development, Testing, Security Audit, Hosting of Dashboard and Mobile Application			
2	Deployment and Maintenance as per terms and conditions for 36 months			
			Total Amount (Bid Value) Rs.	
Total Bid Value in words: Rs.				

The quoted rates include all the charges payable in full compliance to the Scope of Work and other terms specified in the RFQ document.

Yours sincerely,

Authorized Signature [In full and Initials]: ________________________________

Name and Title of Signatory: ____

Name of Firm: ____

Address: ____

Location: ______________________________________Date: _______________

FORM – 6: FORMAT FOR SUBMISSION OF BID SECURITY

[OntheLetterHeadoftheBiddingOrganization]

Date:…..........................

To,

Director and Group Head (IE),
National Productivity Council,
Utpadakata Bhawan,
Lodhi Road,
New Delhi – 110003

Dear Sir,

Sub: Bidders Declaration in respect of EMD for Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three years.

1. I__beingdulyauthorizedtopresentandacton behalf ofM/s... (insertname of Bidding Organization) (hereinafter called the "Bidder") and having read and examined in detail the Bid Document, the undersigned herebyagreethefollowing:
2. We, ...(insert name of Bidding Organization) are submitting the Bid for Design, Development, deployment, Testing, Security Audit, Hosting of Dashboard and Mobile Application and its Maintenance up to three yearsin response to the tender dated…………, issued by National Productivity Council,as per the terms of the Bid Document.
3. We, ...(InsertnameofBidding Organization) are submittingthisEarnestMoneyDeposit(EMD) amount of Rs. 1,00,000/- and agree that any bid not accompanied by the required bid security (EMD) would not be opened.
4. Weagreethat .... (insertnameofBiddingOrganization) in case thebidiswithdrawn

   or

   Modifiedduringtheperiodofitsvalidityorif

   (insertnameofBiddingOrganization) fail to sign the contract in case the work is awarded to us or fail to submit a performance securitybefore the deadline defined in the Bid Document/ letter of award, then …………. (Insert name ofBidding Organization) wouldbe suspended for participating in the bidding process of NPC, for aperiodof three(03)yearsfrombid due date ofabove referred tender.

For and on behalf of Bidding Organization
M/s…………………………………
(Signatureofauthorizedsignatory)

Date: …………………………	Name: ………………………………………
Place: …………………………	Designation: ………………………………