Tender document No: IT/02/CCTV/2024/4093 dated 28.10.2024

TENDER DOCUMENT
FOR
IMPLEMENTATION OF CENTRALIZED UNIFIED COMMAND & CONTROL PLATFORM BASED SECURITY SOLUTIONS AT OMFED DIARY, ARILO, CUTTACK

(through e-tendering)

Table of Contents

THE ODISHA STATECO-OPERATIVE MILK PRODUCERS' FEDERATION LTD-2,
SAHID NAGAR, BHUBANESWAR
PHONE: 0674 – 2546030/ 2546121/2540417 FAX NO: 0674 – 2540974
Website: www.omfed.com E-mail:omfed@yahoo.com

E-Procurement notice

Tender document No.: IT/02/CCTV/2024/4093 dated 28.10.2024

1.	Work name	Implementation of Centralized Unified Command & Control Platform Based Security Solutions at OMFED Diary, Arilo, Cuttack
2.	Availability of tender documents on the e-tendering portal of Government of Odisha	Date: 28.10.2024; Time: 06:30 P.M
3.	Last date for sending queries to OMFED	Date: 01.11.2024; Time: Till 05:30 PM queries may be sent by email to **omfed@yahoo.com**
4.	Pre-bid meeting	Date: 04.11.2024; Time: 03:30 P.M; Venue: Virtual mode
5.	Issue of responses to pre-bid queries, addendum / corrigendum, if required	Date: 06.11.2024
6.	Bid Due Date	Date: 11.11.2024; Time: 03:30 P.M
7.	Opening of Technical Bid	Date: 11.11.2024; Time: 05:00 P.M
8.	POC / Presentation	To be informed to Technically Pre-Qualified Bidders
9.	Opening of Price Bid	To be informed to Technically Qualified Bidders
10	Tender Paper Fee nonrefundable) including GST	Amount: INR 11,800 /- (Rupees Eleven Thousand Eight Hundred only) including GST@18%
11.	Earnest Money Deposit (EMD)	Amount: INR 2,00,000 (Rupees Two Lakh only)

All other details can be seen from the Tender Document available on the e-procurement portal of the Government of Odisha (www.tendersodisha.gov.in) and on the website of OMFED

(www.omfed.com). OMFED reserves the right to reject any or all bids without assigning any reason thereof.

Sd/-

Managing Director

OMFED

www.omfed.com

THE ODISHA STATE CO-OPERATIVE MILK PRODUCERS' FEDERATION LTD.
OMFED, D-2, Sahid Nagar, Bhubaneswar – 751007
Tel. No. 0674-2546030, 2546121, 2540576
E-mail Id: omfed@yahoo.com

Tender Notice

OMFED invites Tender for **Implementation of Centralized Unified Command & Control Platform Based Security Solutions at OMFED Diary, Arilo, Cuttack**.

Interested bidders may submit their offers latest by 03:30 P.M. dt. 11/11/2024. The cost of tender paper is ₹11,800/- (incl. GST 18%) along with EMD of ₹2,00,000/- (Rupees Two Lakh Only) to be submitted online on the e-tender portal of Government of Odisha (www.tendersodisha.gov.in) in favor of OMFED payable at Bhubaneswar. For details visit out official website: www.omfed.com.

The corrigendum / amendment to this notice, if required shall be published only in the OMFED web site and will not be published again in newspaper.

OMFED reserves the right to accept or reject any or all the tenders or part thereof without assigning any reason.

Sd/-
Managing Director

1. Schedule for the Tender

Sl. No.	Parameter	Details
1.	Date of publication of Tender	Date: 28.10.2024 Time: 06:30 PM
2.	Availability of tender documents on the e-tendering portal of Government of Odisha & on the OMFED Website	Date: 28.10.2024 Time: 06:30 PM
3.	Last date for sending queries to OMFED	Date: 01.11.2024; Time: Till 05:30 PM queries may be sent by email to **omfed@yahoo.com**
4.	Pre-bid meeting	Date: 04.11.2024; Time: 03:30 P.M; Venue: Virtual & Will be intimated by mail
5.	Issue of responses to pre-bid queries, addendum/ corrigendum, if required	Date: 06.11.2024
6.	Bid Due Date	Date: 11.11.2024; Time: 03:30 P.M
7.	Opening of Technical Bid	Date: 11.11.2024; Time: 05:00 P.M
8.	POC / Presentation	To be informed to Technically Pre-Qualified Bidders
9.	Opening of Price Bid	To be informed to the Technically Qualified Bidders by appropriate means

OMFED

The Orissa State Cooperative Milk Producers' Federation Ltd.
D-2, Saheed Nagar, Bhubaneswar-751007.
Phone No: 0674-2544576, 2546030, 2546121, 2540417, 2540273
Customer Care Telephone No.- 0674-2547119,
Fax: 0674-2540974 Email Id: **omfed@yahoo.com**

2. DATA SHEET

Sl. No.	Parameter	Details
1.	Name of tender	Implementation of Centralized Unified Command & Control Platform Based Security Solutions at OMFED Diary, Arilo, Cuttack
2.	Type of tendering	Open tendering
3.	Mode of tendering	e-tender
4.	E-tender site	www.tendersodisha.gov.in
5.	OMFED Website	http://omfed.com/
6.	Tender Paper Fee (non-refundable) including GST	INR 11,800 /- (Rupees Eleven Thousand Eight Hundred only) including GST@18%
7.	Earnest Money Deposit (EMD)	INR 2,00,000 /- (Rupees Two Lakh only)
8.	Amount of Performance Security	10% of the total Contract value (excluding taxes) amount shall be submitted in the shape of DD or Bank Guarantee in the format provided in **Annexure-7**
9.	Nodal Officer	Name: Sri. Jitendra Kumar Barada, In-charge (IT) Phone No.: 0674-2546030/ 2546121/2540417 Email: jitendrabarada@omfed.com
10.	Address of OMFED	OMFED, D-2, Sahid Nagar, Bhubaneswar - 751 007 Odisha, India
11.	Tender document No	**IT/02/CCTV/2024/4093** dated 28.10.2024

3. Disclaimer

3.1 This Tender document is neither an agreement nor an offer by OMFED to the prospective Bidders or any third party. The purpose of this Tender document is to provide interested parties with information to facilitate the formulation of their Bid pursuant to this Tender document.

3.2 This Tender document includes statements, which reflect various assumptions and assessments arrived at by OMFED. Such assumptions, assessments and statements do not purport to contain all the information that a Bidder may require. This Tender document may not be appropriate for all persons, and it is not possible for OMFED to consider the particular needs of each party who reads or uses this Tender document. The assumptions, assessments, statements and information contained in the Tender document may not be complete, accurate, adequate or correct. Each Bidder must, therefore conduct its own due diligence and analysis and should verify the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this Tender document and obtain independent advice from appropriate sources.

3.3 Information provided in this Tender document to the Bidder(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information provided is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OMFED accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

3.4 OMFED, its employees make no representation or warranty and shall have no liability to any person including any Bidder under any law, statute, rules or regulations, the law of contract, tort, principles of restitution or unjust enrichment or otherwise for any loss, damage, cost or expense which may arise from or be incurred or suffered in connection with this Tender document, or any matter deemed to form part of this Tender document, or arising in any way in relation to this Bidding Process.

3.5 Neither OMFED nor its employees make any representation or warranty as to the accuracy, reliability or completeness of the information in this Tender document. OMFED also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this Tender document.

3.6 The Bidder should confirm that the Tender document downloaded by them is complete in all respects including all annexures and attachments. In the event the document or any part thereof is mutilated or missing, the Bidder shall notify OMFED immediately in writing.

3.7 If no intimation is received within the last date for submission of Pre-Bid queries, it shall be considered that the Tender Documents received by the Bidder is complete in all respects and that the Bidder is fully satisfied with the Tender Documents.

3.8 No extension of time shall be granted to any Bidder for submission of its Bid on the ground that the Bidder did not obtain the complete set of Tender Documents.

3.9 This Tender document and the information contained herein are strictly confidential and Privileged and are for the exclusive use of the Bidder to whom it is issued. This Tender document shall not be copied or distributed by the recipient to third parties (other than, to the extent required by Applicable Law or in confidence to the recipient's professional advisors, provided that such advisors are bound by confidentiality restrictions at least as strict as those contained in this Tender document). In the event after the issue of the Tender document, the recipient does not continue with its involvement in the Bidding Process for any reason whatsoever, this Tender document and the information contained herein shall be kept confidential by such party and its professional advisors at all times.

3.10 OMFED may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the statements, information, assessment or assumptions contained in this Tender document at any time during the Bidding Process. All such changes shall be uploaded on the website of OMFED. It is the duty of Bidders to visit the website of OMFED regularly and keep themselves updated on the Bidding Process and any communication made in relation to the Bidding Process.

3.11 The Bidders or any third party shall not object to such changes/ modifications
/additions/alterations as provided in **Clause 3.10** above, explicitly or implicitly. Any such objection by the Bidder shall make the Bidder's Bid liable for rejection by OMFED. Further objection by any third party shall be construed as infringement on confidentiality and privileged rights of OMFED with respect to this Tender document.

3.12 The Bidder shall not make any public announcements with respect to the Bidding Process, this Tender document and/or the Bidding Documents. Any public announcements to be made with respect to the Bidding Process or this Tender document shall be made exclusively by OMFED. Any breach by the Bidder of this Clause shall be deemed to be in non-compliance with the terms and conditions of this Tender document and shall render the Bid liable for rejection. OMFED's decision in this regard shall be final and binding on the Bidder.

3.13 By responding to the Tender document, the Bidder shall be deemed to have confirmed that it has fully satisfied and has understood the terms and conditions of the Tender document. The Bidder hereby expressly waives any and all claims in respect thereof.

3.14 The Bid is not transferable.

4. Scope of Services

This Scope of Work outlines the design, procurement, installation, integration, testing, and commissioning of a Unified Command & Control (UCC) Platform-based CCTV Security Surveillance System for the Arilo Dairy, Cuttack, OMFED. The system will include advanced integrated features such as access control, Automatic License Plate Recognition (ANPR/ALPR), perimeter intrusion detection, and AI/ML-based video analytics. It is aimed at enhancing security, monitoring employee behavior, and ensuring operational efficiency.

4.1 Unified Command & Control (UCC) Platform Implementation

4.1.1 **Platform Overview:** Centralized open software capable of managing and integrating all components of the CCTV Security Surveillance System, Access Control, ANPR/ALPR, and AI/ML analytics from a **single platform** for efficient management and operation.

4.1.2 **Key Features:**

i) Real-time monitoring of all connected cameras and sensors.

ii) Centralized dashboard for live video feeds, alerts, and event reporting.

iii) Role-based access control for different user levels (operators, supervisors, administrators).

iv) Incident management and report generation.

v) Scalability to accommodate future expansion.

4.2 High-Resolution EDGE AI CCTV System

4.2.1 **Fixed and PTZ Cameras:**

i) **Coverage:** Strategic installation at key points such as entrances/exits, production areas, storage zones, employee break areas, and perimeter boundaries.

ii) **High-Resolution Imaging:** Minimum 4K cameras for clear imaging in both day and night conditions (IR/night vision).

iii) **PTZ Cameras:** For real-time perimeter surveillance and tracking of intrusions with 360-degree coverage and zoom capabilities.

iv) **Recording and Archiving:** Continuous video recording with at least 90 days of storage, and options for long-term archival.

4.2.2 Ensure the cameras are capable of **24x7 surveillance** and integration with the UCC platform for centralized management.

4.3 Control Room Setup

4.3.1 Design and implement a **state-of-the-art Control Room** equipped with a **video wall** to view live and recorded footage from the entire system.

4.3.2 Provide a **power backup solution** to ensure uninterrupted operation of the control room during power outages.

4.4 Access Control System:

4.4.1 **Entry/Exit Points:** RFID, Biometric, or Smart Card-based access control at all employee and visitor entry points.

4.4.2 **Employee Attendance Management:** Integration with the existing attendance system to ensure automated employee check-ins/check-outs.

4.4.3 **Alarm Triggers:** In case of unauthorized access attempts, the system will trigger alarms to the command center.

4.4.4 Integrate the access control system into the UCC platform for **centralized monitoring** and control.

4.5 Automatic Number/License Plate Recognition (ANPR/ALPR) System:

4.5.1 **Vehicle Monitoring:** Installation of ANPR/ALPR cameras for automatic capture of license plate details of all vehicles at entry and exit points and weigh bridges for errorless integration into respective applications.

4.5.2 **Vehicle Movement Tracking:** Real-time tracking of vehicle movements within the plant premises.

4.5.3 **Whitelisting and Blacklisting:** Authorized vehicles can be pre-registered, and any unauthorized vehicle entries will trigger alerts.

4.5.4 **Event Logs:** Storing vehicle entry/exit records for review and reporting purposes.

4.5.5 Integrate the ANPR/ALPR system into the UCC platform.

4.6 Perimeter Intrusion Detection:

4.6.1 **PTZ Cameras:** Installed along the perimeter of the dairy plant to detect unauthorized access or suspicious activity.

4.6.2 **Motion Detection & Tracking:** Cameras equipped with motion sensors to trigger alerts in the command center upon detecting movement near the perimeter.

4.6.3 **Automated Incident Management:** Any detected intrusion is automatically tracked by PTZ cameras, and operators are alerted to take appropriate action.

4.7 Public Announcement (PA) System:

4.7.1 Install an **IP-based Public Announcement System** at strategic points in the plant.

4.7.2 Integrate the PA system into the UCC platform, allowing announcements to be made from the control room.

4.8 Variable Digital Display Boards:

4.8.1 Integrate **variable digital display boards** around the plant into the UCC platform, allowing real-time communication with staff and visitors.

4.9 SIP Communications and Mobile Camera App:

4.9.1 Provide **SIP-based communication systems** for easy communication between staff and the control room.

4.9.2 Develop and integrate a **mobile camera app** to stream footage from mobile devices directly into the UCC platform for real-time monitoring.

4.10 Integration of Existing CCTV Feeds:

4.10.1 Securely integrate **existing CCTV cameras** into the UCC platform,

ensuring data protection from **cyber threats** and preventing **data leakage**.

4.11 Incident Management Module:

4.11.1 Implement an **incident management module** within the UCC platform for prompt action during emergencies such as:

i) Accidents

ii) Unauthorized access

iii) Fires or smoke

iv) Unruly behavior or fights

4.11.2 Enable notifications, alarms, and alerts to be generated and displayed on the **dashboard** for swift response by field responders.

4.12 Advanced AI and ML-Based Video Analytics:

4.12.1 Provide an **AI/ML-based video analytics platform** integrated with the CCTV system for:

i) **Video synopsis** and **quick search** capabilities.

ii) **Real-time health monitoring** of cameras, sensors, and other IoT devices.

4.12.2 **Hygiene Compliance:** Real-time monitoring of employees for compliance with hygiene regulations, such as handwashing, mask usage, and sanitation in designated areas.

4.12.3 **PPE Kit Compliance:** AI-based detection of Personal Protective Equipment (PPE) such as helmets, gloves, and vests. The system generates alerts for non-compliance.

4.12.4 **Unruly Behavior Detection:**

i) **Behavioral Analysis:** AI-based algorithms to detect suspicious behavior patterns such as unauthorized gatherings, aggressive behavior, or unsafe actions.

ii) **Real-Time Alerts:** Automated notifications to the security command center for immediate investigation and action.

4.12.5 **Reporting & Analytics:** Generation of reports on hygiene and PPE compliance, attendance irregularities, and recorded incidents of unruly behavior.

4.13 Third-Party Application Integration:

4.13.1 Provide integration support for **third-party applications**, including:

i) **SAP/ERP systems**

ii) **Logistic management systems**

iii) **Map services**

iv) **Social media platforms**

v) **Mobile applications**

4.13.2 Facilitate data correlation for **quick and informed decision-making**.

4.14 Future Expansion Capabilities:

The UCC platform must be **scalable** and support future expansion, including:

4.14.1 **Vehicle tracking systems** for milk pickup and product distribution.

4.14.2 **Automation systems** for milk unloading and finished product loading.

4.14.3 **RFID-based crate monitoring** systems.

4.14.4 Detection and prevention of **pilferage** across the product life cycle.

4.15 Unlimited Camera and Server Connectivity:

4.15.1 Ensure the UCC platform is capable of supporting **unlimited cameras, recording servers, and client connections** across multiple sites.

4.15.2 All components should be easily accessible through a **centralized management server**.

4.16 Mobile App and Website Access:

4.16.1 Enable **remote access** to live and recorded footage through a **mobile app** and **website** interface for authorized users.

4.17 Video Recording and Storage:

4.17.1 Ensure all cameras record footage **24x7** in HD resolution or better for a minimum of **60 days**, with the option to extend storage to **90 days** or more.

4.18 Simultaneous Viewing and Control:

4.18.1 Facilitate the **simultaneous viewing** of live and recorded footage by multiple authorized users without degrading the video quality.

4.18.2 Enable control of all cameras and subsystems from the UCC platform.

4.19 Centralized Command and Control Room:

4.19.1 Ensure all surveillance feeds from different locations are sent to the **Centralized Command and Control Room**.

4.19.2 The control room will include a **video wall** displaying a specified number of camera feeds simultaneously.

4.20 Installation & Commissioning:

4.20.1 **Site Survey:** A comprehensive site survey must be conducted to identify camera locations, access points, and perimeter zones.

4.20.2 **Installation:** All cameras, access control devices, and ANPR/ALPR systems must be installed in accordance with the approved site plan. Cabling, network setup, and power backup systems must also be installed to ensure uninterrupted operation.

4.20.3 **Testing:** Comprehensive system testing including camera functionality, access control integration, ANPR/ALPR accuracy, perimeter intrusion detection, and AI/ML analytics performance.

4.20.4 **Commissioning:** Once testing is complete, the system will be commissioned for use and handed over to the plant security team.

4.21 Training & Documentation:

4.21.1 **Training:** Provide training to the plant security personnel and system operators on how to use the UCC platform, monitor video feeds, manage access control, and respond to incidents.

4.21.2 **User Manuals:** Detailed user manuals and operational guides for system components must be provided.

4.21.3 **Maintenance Guides:** Documentation on system maintenance, troubleshooting, and periodic testing schedules.

4.22 Maintenance & Support:

4.22.1 Provide **Operation and Maintenance (O&M)** services for the entire system for **five (5) years** from the date of commissioning.

4.22.2 The O&M services will include regular updates, troubleshooting, and system optimization.

4.22.3 **24/7 Support:** Availability of 24/7 remote technical support and on-site support as needed.

4.23 Deliverables:

4.23.1 Fully functional and integrated Unified Command & Control-based CCTV Security Surveillance System.

4.23.2 AI/ML-powered video analytics for Quick Search, Video Synopsis, Health monitoring of devices, monitoring employee behaviour, hygiene, and PPE compliance.

4.23.3 Automated vehicle monitoring with ANPR/ALPR for entry, exit, and movement tracking.

4.23.4 Perimeter intrusion detection system with PTZ cameras.

4.23.5 Access control system integrated with the UCC platform.

4.24 This detailed Scope of Work outlines the essential requirements for a comprehensive, future-proof, and scalable **UCC Platform-based CCTV Security Surveillance System** for the Arilo Dairy Plant, OMFED. The solution will enhance security, operational efficiency, and safety within the plant premises while integrating state-of-the-art technologies to meet current and future demands.

4.25 The BOQ for Arilo Dairy is mentioned below:

Unified Command & Control based Security Solution at Arilo Dairy (Phase-1)			
Sl. No.	**Description**	**UOM**	**Qnty**
1	Management Server with Microsoft server 2022 std. license	Nos	1
2	Primary NAS Storage 12 Bay, 8 nos. X 12 TB HDD with redundant power supply	Nos	1
3	Workstation with Core i7 12th Generation, 32 GB RAM, 6 GB Graphics card & windows 11 Professional	Nos	2
4	21.5'' Monitor Full HD	Nos	2

5	Core Switch -L3 24 Port Switch Fully Managed with 16 Copper + 8 SFP Ethernet Port	Nos	1
6	L2 Fully Managed 8 Port Giga PoE Switch poe Output with 2 SFP Port.	Nos	19
7	IP 5 MP dome Camera POE Supported UL Certified with mounting accessories	Nos	50
8	IP 5 MP Bullet Camera motorised varifocal Lense POE Supported UL Certified with mounting accessories	Nos	10
9	4MP IP PTZ camera IR 200 mrt motorised varifocal Lense POE Supported UL Certified with mounting accessories	Nos	3
10	ANPR/ALPR camera- Edge based AI ML camera UL Certified with Industrial Grade Giga POE++ Injector and mounting accessories	Nos	2
11	12 port LIU with loaded	No	20
12	SC-LC Patch Cord	Nos	42
13	1000 Base 1310nm SM Transceiver Module	Nos	42
14	Cat 6 factory made patch cord 3 Mtr	Nos	20
15	Cat 6 double jacketed UTP Outdoor Cables	Box	5
16	Optical fibre cable -6 core, Single Mode, Armoured	mtrs	500
17	CCTV Dual/Triple Cantilever Galvanized Pole, Civil Foundation with Proper Chemical Earthing	Nos	3
18	Water & Dust proof Camera Back box	Nos	70
19	1 KVA UPS Internal Battery Cables etc.	Nos	19
20	10 KVA Online UPS with External Battery Rack, Cables etc.	Nos	2
21	65" 4K HDR Professional Display with mounting accessories	Nos	2
22	98" 4K HDR Professional Display with mounting accessories	Nos	1
23	Micro Data Center, with 24U Indoor rack, 1 kW Panel AC cooling, 230V, 50/60 Hz, 1300H x 1060W x	Nos	1
24	RJ 45 Connector industrial Grade	pkt	2
25	Outdoor IP Horn/Speaker for PA system with all Accessories	Nos	5
26	Electric power cable with Field Location Electrical Work-All type(Approx.)	Lot	1
27	SPD (Surge Protection Device) Unit	Nos	20
UNIFIED COMMAND & CONTROL SOFTWARE			
28	Integrated & unified command and control software with Video management software (VMS), GIS engine, PA (Public announcement application, Parking management application plugin, Realtime alert/ alarm, threat level & management Engine, Mobile & Web applications. with UL certification	Nos	1
29	Camera connection Licence with Advantage 5 Year support service	Nos	63
30	ANPR/ALPR Camera Connection Licence with Advantage 5 Year support service	Nos	2

31	PA system -IP horn connection license with Advantage 5 Year support service	Nos	5
Service			
32	6 U Rack with all accessories installation	Nos	19
33	OFC - 6 Core SM-Type Armoured cable with Laying, Termination accessories	Mtr	4000
34	Cat 6 UTP Cables Indoor with laying PVC pipe	Mtr	3660
35	Site Survey, Planning, Designing, Civil Work, Installation, Commissioning, Testing & Training of the complete system	Lot	1
Items with OMFED			
36	OFC Cables 6 Core	Mtr	1400
37	Internal CAT6 Cables 305 Mtr Bundle	Nos.	12
38	6U Wall Mount Rack	Nos.	38
39	42U Server Rack	Nos.	01

4.26 The SI shall complete the activity at Arilo Dairy, Cuttack within 08-12 Weeks from the date of signing of agreement.

4.27 The detailed scope and specifications of the services, along with the contract period, payment terms, etc. are given in Special Conditions of Contract as enclosed in **Annexure-2**.

4.28 The "General Conditions of Contract-Services" as enclosed in the tender at **Annexure-1** shall form an integral part of the Tender document and will also form a part of the Agreement placed against this tender.

5. Eligibility Criteria

The technical evaluation of bidders will be conducted based on the following parameters. Offers from firms not conforming to any of these criteria will be rejected:

Sl. No.	Criteria	Required Documents
5.1	**Technical Criteria** The bidder must have at least 5 years of experience in implementing minimum 3 nos of IP-based CCTV systems, and Command & Control software solutions, including integration with 3rd party video analytics software for an aggregate value of ₹10 Crore. **Note:** a. "Similar completed Services" shall mean the Bidder should have successfully executed the work of supply, installing, testing, commissioning and maintenance of Command & control software based security surveillance system in a government organization (at Central government /State government/ PSU/ government Undertaking). b. Applicable 5 (Five) years shall be preceding five financial years excluding the financial year of floating of the Tender (i.e. FY 2019-20 to FY 2023-24)	As per the **Annexure-2C** Self-attested copies of a) Relevant contracts or work orders or agreements containing the scope of services, the value of the contract or work order or agreement; and b) Completion certificate from their clients/employers, regarding successful completion of the services. c) In case value of the contract is not mentioned in the contract or work order or agreement, then the value must be mentioned in the completion certificate issued by the client/employers.
5.2	**Financial Criteria** The bidder must demonstrate an average annual turnover of no less than ₹10 Crore over the last three financial years i.e. 2021-22, 2022-23, and 2023-24.	a) Average Turn Over certificate of last 03 years (Year wise turnover) certified by Charted Accountant. b) Copies of audited financial statements. c) 26 AS Form for respective financial years shall be submitted.
5.3	Other Criteria	
5.3.1	The bidder must be a registered entity under one of the following: 1. Indian Companies Act, 2013 2. Indian Partnership Act, 1932 3. Limited Liability Partnership Act, 2008 4. Proprietorship Firm The bidder should have been	Copies of a) Company (Private or Public) • Certificate of Incorporation • Memorandum of Association • Articles of Association b) Registered partnership firm • Registration certificate • Deed of Partnership

	registered for a minimum of 10 years as of March 31, 2024.	c) LLP firm • Certificate of Incorporation • Deed of Partnership
5.3.2	The Bidder should have valid P. Tax, PAN and GSTIN registration	• Copy of PAN & P.Tax certificate • Copy of GST registration certificate
5.3.3	The Bidder should not have been banned / blacklisted by OMFED or any government agency or any PSU as on the date of submission of Bid	Affidavit to this effect, as per the format given in **Annexure-4**
5.3.4	Tender Paper Fee, EMD amount and Power of Attorney	a) Proof of Payment of Tender Paper Fee; please refer to **Clause 7.6** for further details. b) Proof of Payment of EMD; please refer to **Clause 7.7** for further details. c) Power of Attorney (as per format given in **Annexure-8**) in favor of the authorized signatory of the bidder. Please refer to **clause 7.5** for further details.
5.3.5	The Bidder whose Contract / Agreement with OMFED had been terminated / Failed to perform will not be eligible to participate in the bidding process.	Decision of OMFED in this regard is final & binding on all such entities
5.3.6	The bidder should have an office located in Odisha. If the bidder does not have a presence in the state, they must provide an undertaking to establish a project office within one month of contract award.	Supporting evidence towards presence in Odisha needs to be submitted. Undertaking on company letter head to be submitted to establish office in Odisha if own the tender.
5.3.7	Bidder / OEM should have own dedicated support center available during working hours and must have at least 01 Service Center in Odisha to Provide onsite support.	Self-Attested copy of Service Center details like detail address to be attached.
5.3.8	Bidders must provide tender-specific Manufacturer's Authorizations (MAF) for key items, including Command & Control software, CCTV, Servers, Storage solutions, Switches, Cables (OFC & UTP), MDC racks, and UPS systems.	Copy of OEM Authorization Certificate on their letterhead to be attached as per the **Annexure-2B** Note: (OMFED may cross verify with the OEM whether Authorization is authenticated or not.)
5.3.9	**Quality Certifications:** The bidder must be certified under ISO 27001:2022, ISO 20000:2018, and ISO	A copy of the valid certificates must be submitted.

	9001:2015.	
5.3.10	Compliance Sheet of all products / Materials to be submitted.	All technical compliance documents must be signed and stamped by the OEM on their official letterhead.
5.3.11	All the products / materials should have 05 years Warranty	Copies of supporting documents from OEM to be attached.
5.3.12	**Product Certification:** All the Cameras and analytics servers must be UL listed, as well as certified by BIS, CE, and FCC.	Copies of necessary certificate by mentioned authorities to be submitted.
5.3.13	**MSME Registration:** The bidder should be a registered MSME unit.	Relevant MSME/NSIC registration documents must be submitted along with the technical bid.
5.3.14	Site Survey report	A Complete report after Physical Site survey to be submitted.
5.3.15	Any influence on any of the employees of the Buyer organization to favor the bidder lead to disqualification of the bidder without notice	
5.3.16	Either the Bidder/OEM or authorized dealer / agents on behalf of the OEM can participate. Both cannot bid for the same Item /product.	
5.3.17	AMC of 5 Years for this project.	MoU to be signed
5.3.18	**Rate contract for 5 years for future enhancements**	**Bidder should submit an authorization for rate contract for all BOQ materials for 5 years to supply and installation with warranty and support for OMFED future enhancement within any area of ODISHA in same price and terms.**

5.4. Note:

a. The value of the contracts or work orders or agreements to be considered shall be exclusive of all taxes and duties.
b. Only completed projects shall be considered as part of experience. Any ongoing, partially completed project shall not be considered as part of any credential and if submitted shall be solemnly rejected.
c. The technical experience as a sub-contractor to a main agency in a project/Contract awarded by the Competent Authority of principal employer shall not be considered towards any qualification criteria.
d. Bidding in the form of a consortium is **NOT** allowed.

5.5. Eligibility and Evaluation Methodology

5.5.1. Eligibility

The eligibility criteria for bidders were outlined earlier. The evaluation process will assess each bidder's relevant qualifications to determine which one best meets the overall project requirements. This evaluation will consider various factors, including the bidder's track record, financial capabilities, customer handling experience, technical bid, price bid, and adherence to commercial terms and conditions.

5.5.2. Preliminary Examination

The Purchaser will conduct a preliminary examination of the bids to ensure they are complete, adhere to the specified bid format, and that all required documents are properly signed. The Purchaser reserves the right to waive any minor informality, nonconformity, or irregularity in a bid, provided it does not constitute a material deviation from the requirements.

During the tendering process, the Purchaser may, if necessary, request clarifications or technical presentations from any or all bidders. The purpose of these clarifications is to resolve ambiguities or uncertainties arising during the evaluation of bid documents. Oral clarifications allow the evaluation committee to clearly communicate its requirements and give bidders an opportunity to further clarify their proposals. The committee may also seek input from professional and technical experts during the evaluation process.

However, bidders will not be permitted to alter the substance of their RFP or modify the quoted prices during the clarification process.

5.5.3. Evaluation methodology

5.5.3.1. Evaluation under Combined Quality-cum-Cost Based System (CQCBS)

Technical Score (Ts):

The technical evaluation will follow a point-based scoring methodology. A panel of experts may be constituted by the TENDERING AUTHORITY to assess the technical presentation. Bidders will be required to make a PowerPoint presentation before the evaluation committee.

** Only bidders who achieve a minimum of 70 marks will be considered technically qualified for the opening of the financial bid.*

Financial Score (Fs):

The bidder with the lowest financial proposal will receive a financial score of 100 points. The financial scores for other proposals will be calculated as follows:

Fs = 100 x (FM1 / F1)

Where:

- F1 = Financial Proposal amount submitted by the bidder
- FM1 = Lowest financial quote

Combined and Final Evaluation:

Proposals will be ranked based on the combined technical (Ts) and financial (Fs) scores, calculated using the formula:

S = (Ts x Tw) + (Fs x Fw)

Where:

- S = Combined score
- Tw = Weight assigned to the Technical Proposal (0.70)
- Fw = Weight assigned to the Financial Proposal (0.30)

The bidder with the highest combined score (First Ranked Applicant) will be selected. The second and third-ranked applicants will be kept in reserve and may be invited for negotiations or engagement under the same terms as the selected agency in the event of withdrawal, failure of the selected agency, an increase in the volume of work, or for any other reason.

5.5.4. Technical Evaluation

5.5.4.1. Evaluation of Technical Proposal

Technical Bid Evaluation Process

The evaluation of the technical bids will be conducted as follows:

1. **Evaluation of Technical Solutions**:
   The technical solutions proposed by bidders in their bid documents will be evaluated in line with the requirements and criteria outlined in this RFP. Bidders must submit all necessary documentation to support the evaluation criteria (e.g., detailed project citations, completion certificates, profiles of project resources, etc.) as specified for the technical evaluation.
2. **Proposal Presentations**:
   The Tender Evaluation Committee (TEC), appointed by the TENDERING AUTHORITY, may invite each bidder to deliver a presentation at a specified date, time, and venue. The purpose of the presentation is to allow bidders to showcase their proposed solutions, emphasizing key points in their proposals and demonstrating how their solutions meet or exceed the requirements set forth in the RFP.
3. **Evaluation of Technical Bids**:
   The technical bids will be opened and evaluated for compliance with the techno-functional requirements, deviations, and overall technical suitability. Bidders must respond comprehensively to the experience, qualifications, and technical requirements outlined in the RFP.
4. **Demonstration Requirement**:
   After the technical bid opening, bidders may be required to demonstrate their surveillance system at the site.
5. **Technical Evaluation Methodology**:
   A. Each technical bid will be scored out of a maximum of 100 points.
   B. Commercial bids of bidders who do not meet the technical qualification criteria or fail to satisfy all technical evaluation requirements will be returned unopened at the conclusion of the evaluation process.
   C. The committee will notify all technically qualified bidders of their technical evaluation results via written communication. Each bidder will be informed of their individual technical score prior to the opening of commercial bids.
   D. Technically shortlisted bidders will be informed of the date and venue for the opening of commercial bids via postal mail, courier, or email.

5.5.5. Evaluation Criteria

The technical proposal shall be evaluated based on the information provided.

Sl. No.	Assessment Parameter	Marks
1	The Bidder Must have minimum 10 Number of Technical Staff under Direct Payroll for early and easy support service. EPF & ESIC Registration certificate with latest challan must be enclosed. i. Minimum 10 Technical Staff - 05 marks ii. Minimum 15 Technical Staff – 10 Marks	10
2	Registered ISO certified (ISO 9001: 2015, ISO 27001 :2022, ISO 20000: 1 2018). i. 1 no of Certificate – 3 Mark ii. 2 nos of Certificates – 6 Mark iii. 3 nos of Certificates -10 mark	10
3	Executed Similar Type of Project (Command & control software based security surveillance system) of Rs. 2 Crore in any state Govt / Central Govt / PSU or any Government undertaking agency. i. 1 no of project- 3 Mark ii. 2 nos of Projects- 6 Mark iii. 3 nos of Projects -10 Mark	10
4	Executed ANPR/ALPR solutions project based on Command & Control Platform in any state / Central Govt /any Govt undertaking Agency. i. Projects of min 10 nos ANPR/ALPR with Performance Certificate- 3 Mark ii. Projects of min 20 nos ANPR/ALPR with Performance Certificate - 6 Marks iii. Projects of min 40 nos ANPR/ALPR with Performance Certificate - 10 Marks	10
5	Average Annual Turnover of Last 3 Years. FY2021-22, 2022-23, 2023-24 i. Average Annual Turnover 10 Crore – 3 Marks ii. Average Annual Turnover 15 Crore – 6 Marks iii. Average Annual Turnover 20 Crore – 10 Marks	10
6	The bidder must have implemented 3rd Party AI Video Analytics tools on a Command & Control Platform and Central Monitoring of more than one remote site in any state/Central Govt/Govt undertaking Agency. i. 3rd Party AI Video Analytics Tools – 5 Marks ii. Central Monitoring of Remote Site – 5 Marks	10
7	The bidder must have completed similar nature of work costing minimum for any single customer in last 5 Financial years with a minimum budget of i. Rs.200.00 lakhs - 3 Marks ii. Rs.500.00 lakhs - 6 Marks iii. Rs.1000.00 lakhs - 10Marks	10
8	The Bidder Must have Authorization from Major OEM's Like CCTV, Switch, optical Fiber cable, LAN Components. And the above OEM must have presence in India from minimum 03 (three) years. i. 03 Years – 03 Marks ii. 05 Years - 06 Marks iii. 10 years - 10 Marks	10
9	Presentation of overall projects Proof of Concept (POC)	20
	Total	100

The cut-off mark for qualification in the technical proposal evaluation is set at 70 points.

The success of this project will rely heavily on the seamless integration of future CCTV surveillance cameras, Command & Control Software, user databases, and eventual integration with other Emergency Response Systems. Therefore, the demonstrated Proof of Concept (POC) capability of the integrated solution will be a critical component of the technical evaluation conducted by the Technical Evaluation Committee (TEC).

5.5.6. Commercial Bid

5.5.6.1. Opening of Commercial Bids

The Purchaser will open the commercial bids of qualifying bidders in the presence of representatives from the bidders who choose to attend. The time, date, and location for the opening will be determined by the Purchaser.

5.5.6.2. Evaluation of Commercial Bids

The Purchaser will evaluate the commercial bids for completeness and accuracy. Any arithmetical errors will be corrected based on the following criteria:

1. If there is a discrepancy between the unit price and the total price (calculated by multiplying the unit price by the quantity), the unit price will take precedence, and the total price will be adjusted accordingly.
2. In cases where discrepancies exist between the written amount and the numerical figures, the amount in words will prevail.

The overall bid price, adjusted as necessary, will be used by the Purchaser for the commercial evaluation of the bids.

6. OEM Eligibility Criteria:

6.1 **CCTV**

Sl No	Description	Compliance (Yes / No)
1	CCTV Camera OEM should not be blacklisted in India or anywhere globally for security reasons from any organization including ONVIF.	
2	OEM Should be ONVIF fulltime member, and the name of the OEM should reflect in the ONVIF site.	
3	The OEM of Camera should have its own company registered in India and having direct presence since last 10 years. Any representation through a dealer / Distributor / Subsidiary / Consortium shall not be treated as OEM. This must be supported by necessary statutory documents. (Certificate of Incorporation)	
4	CCTV OEM should have manufacturing in India since last five years or Foreign CCTV OEM should have manufacturing unit globally from last 10 years. Documentary evidence should be submitted.	
5	The Camera OEM should be a Genuine Manufacturer and should have official valid H.265 HEVC certificate and should be listed on HEVC website at the time of submitting the bid. The same will be checked through official website (i.e. https://www. mpegla.com/programs/hevc/licensees/)	
6	The CCTV Camera OEM should submit a declaration that any of the proposed cameras not contain any “HiSilicon make chipset / SoC / Sensor / Any other Low end chip manufacturer with Security issues	

	/parts. The declaration needs to be on OEM letter head regarding quoted model specific sensor and SoC details like Make, Model etc.	
7	OEM should have its own Service Centers & Repairing Center in Odisha in their own Name. This should be supported with necessary documentary evidence.	
8	CCTV OEM Company should not be technically rejected in any Govt. tender in India for their origin from any land border sharing countries of India.	
9	OEM Should be CE, FCC, ROHS, UL Required.	
10	The MAC address of the cameras must be registered in the name of the OEM supplying them.	

6.2 Network Switches

Sl No	Description	Compliance (Yes / No)
1	OEM should have ISO9001:2015 certified or similar certificate.	
2	OEM should have ISO/IEC 27701:2019 certified or similar certificate.	
3	OEM should have valid NSCS Certificate from Trusted Telecom Portal.	
4	The OEM should have MTCTE certified from day 1	
5	OEM Should Be Minimum CMMI Level III or Equivalent.	
6	OEM should have presence in INDIA for more than 5 years.	
7	Technical compliance Must be provided on OEMs letterhead with due details (signatures, name, email, contact number of Authorized signatory)	
8	Quoted product should have support centre in India.	
9	The OEM Should Have FCC/IEC/CE Certification	

6.3. Passive Components

S.No.	Description	Compliance (Yes / No)
1	The OEM of Passive Network Components should be present in the India for at least last 10 Years. (Document proof Required - Proof of Incorporation should be attached)	
2	Should have Technical / Telephonic support center in India	
3	OEM must have ISO 9001:2015, ISO 14001:2015 and ISO 45001:2018 or latest	
4	Factory Test report must be provided for the product during supply.	
5	All the components /raw materials used must be RoHS-verified	
6	OEM should have its Manufacturing units, Components and Finished Goods Warehouse & R&D labs in India.	
7	OEM should have at least four dedicated Presales manpower in India. for after sales support	
8	25-year Performance warranty; Warranty to cover Bandwidth of the specified and installed cabling system	
9	The entire passive components Copper and fiber should be from a Single OEM of one make.	
10	The Proposed OEM should be a member of BICSI and should have a certified project management professional (PMI-PMP®) and a CDCP®	

	/ RCDD® on the OEM's payroll sitting in India whose services can be utilized for this project. Valid Certificates of the OEM employees along with a letter from the OEM HR Department verifying that the employees are in fact sitting in India should be submitted. (Details must be provided).	
11	Products Should be ETL channel performance verified on a 04-Connector channel or more, tested upto 350Mhz or more with an MTPL Plug as per ANSI/TIA-568.2-D (Part Code to be mentioned in report and should be submitted along with bid) and UL Listed (Relevant Document to be shared)	
13	The OEM shall be recognized by the Department for Promotion of Industry and Internal Trade under the 'Telecommunication & Networking' Industry and 'Network Technology Solutions' sector by Government of India.	
14	Quoted product part numbers must be available on OEM's official website	

7. Instruction to Bidders

7.1 The Bidders intending to participate in this tender are required to register on the e-procurement portal of the Government of Odisha (www.tendersodisha.gov.in.). This is a onetime activity for registering on the Government website. During registration, the Bidders will be required to attach a Digital Signature Certificate (DSC) to the Bidder's unique user ID. The DSC used should be of appropriate class (Class II or Class III) issued from a registered Certifying Authority. The registration of Bidders on the portal shall be free of cost. The registration shall be in the name of the Bidder, whereas the DSC holder shall be the duly Authorized Signatory of the Bidder.

7.2 The tender documents shall be available on the state e-procurement portal (www.tendersodisha.gov.in) and the website of OMFED (www.omfed.com). There shall be no sale of hard copies of the tender documents. Tenders can be accessed by the prospective Bidders at the above websites and may be downloaded by them free of cost. However, the Tender Paper Fee shall have to be paid at the time of bid submission, unless exempted to be paid by the competent authority.

7.3 E-tendering process is mentioned in **Chapter 09**.

7.4 The bids are to be submitted in two covers, consisting of: (i) Technical Bid (under Cover I) and (ii) Price Bid (under Cover II). Both the Technical Bid and the Price Bid have to be submitted on the e-procurement portal of the Government of Odisha.

7.5 The Authorized Signatory of the Bidder shall be duly authorized by a Power of Attorney authorizing him/her to perform all tasks related to tender submission, including but not limited to sign and submit the bid and to participate in the bidding process on behalf of the Bidder. The format for the Power of Attorney is given in **Annexure-8** of this Bid document. Each page of all scanned documents submitted as part of the Technical Bid shall be initialed with date by the Authorized Signatory of the Bidder at the lower left-hand corner of each page. The power of attorney is

case of company shall submit the board resolution in this regard.

7.6 Tender Paper Fee

7.6.1 The Bidder shall pay to OMFED a non-refundable amount ("Tender Paper Fee"), indicated in the Data Sheet, as part of its Technical Bid. The mode of payment of the Tender Paper Fee is also indicated in the Data Sheet.

7.6.2 The Bidders, who are exempted to deposit Tender Paper Fee due to any exemption granted by the Government of Odisha, are required to attach scanned copy of relevant documents evidencing such exemption granted, along with the Technical Bid document while submitting online. The Bidders, who does not submit Tender Paper Fee claiming exemption but does not submit relevant document, is ineligible for bidding and such bid shall be summarily rejected.

7.7 Earnest Money Deposit (EMD)

7.7.1 Bidders as part of their Technical Bid shall have to submit an Earnest Money Deposit; the amount of the EMD as indicated in the Data Sheet.

7.7.2 **Mode of Payment:** The EMD shall be in the form of DD and in favour of OMFED, Bhubaneswar payable at Bhubaneswar. The mode of submission of the EMD is also indicated in the Data Sheet. For the avoidance of doubt, it is clarified that OMFED shall not be liable to pay any interest on the EMD deposit so made and the same shall be interest free.

7.7.3 **EMD Exemption:** MSME Registered bidders are exempted on EMD. The bidders who are exempted to deposit Earnest Money Deposit (EMD) are required to attach copies of relevant documents evidencing such exemption granted, along with the Technical Bid document while submitting. The Bidders, who does not submit EMD Fee claiming exemption but does not submit relevant document, is ineligible for bidding and such bid shall be summarily rejected.

7.7.4 **Return of EMD:**
The EMD of the technically disqualified Bidders shall be returned after declaration of the list of technically qualified Bidders. The EMD of other unsuccessful Bidders shall be refunded after signing of the Agreement with the Successful Bidder. The return of the EMD shall be in the form of bank transfer to the account of the Bidder by OMFED.

7.7.5 The EMD of the Preferred Bidder shall be returned upon the Preferred Bidder furnishing the Performance Security.

7.7.6 **Forfeiture of EMD:** The EMD shall be forfeited and appropriated by OMFED as a genuine pre-estimated compensation and damages payable to OMFED for, inter alia, the time, cost and effort of OMFED without prejudice to any other right or remedy that may be available to OMFED hereunder, or otherwise, under the following conditions:

i) if any of the documents submitted by a Bidder as part of the bid is found to be not genuine or forged or any of the claims, confirmations, statements or declarations of the Bidder is found to be incorrect or inconsistent, or is a case of any material misrepresentation of facts at any point of time during the bid evaluation process;

ii) if the Preferred Bidder fails to acknowledge and return to OMFED a signed copy of the LoA or Agreement within the timeframe allowed by OMFED;

iii) if the Preferred Bidder fails to submit the Performance Security within the timeframe allowed by OMFED;

iv) if a Bidder withdraws its bid before completion of the bidding process during the bid validity period, except as provided in **Clause 7.8**;

v) If the Bidder has otherwise committed any breach of the terms of this Bid document;

vi) in case the Preferred Bidder, does not comply with the requirements of the Price Bid;

vii) in case the Technical Bid of a Bidder contains any information on the Price Bid of the Bidder;

7.7.7 In case of cancellation of the tender before bid opening date and time, the EMD shall be refunded to respective Bidder's account.

7.8 Bid validity period: The bid shall initially remain valid and binding on the Bidder for at least Five Years (05 Years) from the Bid Due Date, as given in the Schedule for the Tender & as mentioned in Section 5 Table point 5.3.17. Any bid with a shorter validity period shall be rejected by OMFED. Under exceptional circumstances, OMFED may in writing request the Bidders to extend the bid validity period of their bids. In case the Bidder refuses the request of OMFED to extend its bid, the EMD of such Bidder will be returned to the Bidder. However, such bids will not be evaluated further.

7.9 Issue of clarifications: Bidders may also send their queries by email; queries received after the last date for sending queries (as per the Schedule for the Tender) may not be considered by OMFED. The responses to the queries received shall be published by OMFED on its website or will be discussed during pre-bid meeting or will be sent through mail and the same shall also be considered to be a part of the tender documents; however, the source of queries shall not be mentioned.

7.10 Issue of corrigendum / amendment: At any time prior to the Bid Due Date, OMFED may at its own initiative or in response to a query or clarification requested by a prospective Bidder if found appropriate, issue a corrigendum/ amendment to the tender documents, which shall be available for download on its website and the same shall also be considered to be part of the tender documents. In order to give Bidders reasonable amounts of time to take into account such corrigendum / amendment, OMFED may at its own discretion also extend the Bid Due Date.

7.11 Extension of Bid Due Date: OMFED may, at its discretion, extend the Bid Due Date which shall be related as an act of amendment of this Bid document.

7.12 Acknowledgement by the Bidder: It shall be deemed that by submitting its bid, the Bidder has:

i) made a complete and careful examination of the tender documents, including the proforma agreement;
ii) received all relevant information requested from OMFED;
iii) accepted the risk of inadequacy, error or mistake in the information provided in the tender documents or furnished by or on behalf of OMFED relating to any of the matters related to this tender or otherwise;
iv) satisfied itself about the scope of work and services to be delivered/rendered and the extant conditions and all matters, things and information necessary and required for submitting an informed bid and for providing the required services in accordance with the tender documents including the contract (to be signed with OMFED) and performance of all of its obligations there under;
v) acknowledged and agreed that inadequacy, lack of completeness or incorrectness of information said to be in the bidding documents or ignorance of any of the matters shall not be a basis for any claim for compensation, damages, extension of time for performance of its obligations, loss of profits etc. from OMFED;
vi) agreed to be bound by the undertakings provided by it under and in terms; and

OMFED shall not be liable for any omission or commission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to the tender documents or the bidding process, including any error or mistake therein or in any information or data given by OMFED.

7.13 **Right to accept or reject any/ all bids**: Notwithstanding anything contained in the Tender document, OMFED reserves the right in its sole discretion, without any obligation or liability whatsoever, to accept or reject any or all of the Bids at any stage of the Bidding Process without assigning any reasons, thereof. Further OMFED reserves the right to annul the Bidding Process and / or to reject any or all Bids at any stage prior to the signing of Agreement without thereby incurring any liability to the affected Bidders or any obligation to inform the affected Bidders of the grounds for OMFED's action. Decision of OMFED shall be final and binding in this regard. OMFED reserves the right to reject any bid if at any time, a material misrepresentation is made or uncovered or if the bid received is conditional or qualified.

7.14 **Language of the bid:** The bid and all related correspondence and documents in relation to the bidding process shall be in the English language. Supporting documents and printed literature furnished by the Bidder with the bid may be in any other language provided that they are accompanied by translations of all the pertinent passages in the English language, duly authenticated and certified by the Bidder. Supporting materials, which are not translated into English, may not be considered. For the purpose of interpretation and evaluation of the bid, the English language translation shall prevail. The English translation of the documents shall be carried out by professional translators and the translator shall certify that he is proficient in both languages in order to translate the document and that the translation is complete and accurate.

7.15 **Bid to be submitted by Bidders:** The bid to be submitted by Bidders shall consist of the Technical Bid and the Price Bid.

7.15.1 **Technical Bid:** Bidders shall have to submit their Technical Bid online in e-Tender Portal. The Technical Bid should consist of clear and legible copies of

all the required documents and should be submitted within the Bid Due Date, as indicated in the Schedule for the Tender. The Technical Bid shall contain no information on the Price Bid of the Bidder. The Technical Bid shall consist of the following:

i) Documents Supporting Eligibility Criteria (**Refer Chapter 5**)

ii) Technical Bid checklist as per **Annexure-5**

iii) Mandate Form for Bank payment as per **Annexure-6**

7.15.2 **Price Bid:** The Price Bid shall be submitted as per the price bid format in **Annexure-3**.

7.16 Material deviation

7.16.1 Bids shall be liable for rejection in case of material deviation, that shall include, inter alia, the following:

i) The Technical Bid or any accompanying document or Price Bid submitted by the Bidder is not in accordance with the formats given in this tender document.

ii) The Technical Bid is not accompanied by all the documents required to be submitted in terms of this tender document as per **Clause 7.15.1**

iii) It does not contain all the information (complete in all respects) as requested in this tender document (in accordance with the formats provided in this tender document);

iv) The Technical Bid is not accompanied by documentary evidence of the credentials of the Bidder(s).

v) The Technical Bid or Price Bid submitted by the Bidder is conditional or qualified.

vi) The bid submitted by the Bidder is not valid for the minimum bid validity period, as per **Clause 7.8**.

vii) It is otherwise substantially/ materially in deviation of the terms and conditions of the tender document.

7.16.2 OMFED may waive any nonconformity in the Bid that does not constitute a material deviation, reservation or omission. OMFED may request that the Bidder submit information or documentation, within a reasonable period of time (**Refer Clause 7.19.3**), to rectify nonmaterial nonconformities in the Technical Bid related to documentation requirements. Requesting information or documentation on such non-conformities shall not be related to any aspect of the Price Bid. Failure of the Bidder to comply with the request of OMFED by the date specified therein, may result in the rejection of its Bid. OMFED, however, is not bound to waive such non-conformity under this **Clause 7.16.2**.

7.17 Bid preparation cost: The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OMFED or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and OMFED shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

7.18 Opening of Technical Bids: The Technical Bids shall be opened as per the schedule indicated in Schedule for the Tender.

7.19 Evaluation of Technical Bids:

7.19.1 The Technical Bids shall first be evaluated to determine whether they are complete, whether the required documents have been submitted in the correct formats and whether the documents have been properly signed by the Authorized Signatory and whether the Technical Bid is generally in order. It will be determined whether the Technical Bid is of acceptable quality, is generally complete and is substantially responsive to the tender documents. For purposes of this determination, a substantially responsive Technical Bid is one that conforms to all the terms, conditions and specifications of the tender documents without any material deviations (as defined in **Clause 7.16**), objections, conditionality's or reservations.

7.19.2 A Technical Bid which is not substantially responsive, may be rejected by OMFED, and may not subsequently be made responsive by the Bidder by correction of the material deviations, as defined in **Clause 7.16**.

7.19.3 If required, OMFED may ask Bidders to provide clarifications on the submitted documents provided in the Technical Bid, if necessary, with respect to any doubts or illegible documents. The Officer Inviting Tender may ask for any other documents of historical nature during Technical Evaluation of the tender. Non submission of legible documents may render the bid nonresponsive. The authority inviting bid reserves the right to accept any additional document. Such clarifications shall be submitted by the Bidder through email. The Bidders shall be allowed a maximum time period of 3 (three) working days for submitting the requisite shortfall documents through email. However, no changes in the Price Bid shall be sought, offered or permitted, nor shall the documents sought be related to the EMD. No modification of the bid or any form of communication with OMFED or submission of any additional documents, not specifically asked for by OMFED will be allowed and even if submitted, they may not be considered by OMFED.

7.19.4 The responsive Technical Bids shall then be evaluated in detail to determine whether they fulfill the eligibility criteria (as given in **Chapter 5**) and other requirements of the tender, such as submission of all the requisite documents as listed in **Clause 7.15.1**.

7.20 Opening and Evaluation of Price Bids

7.20.1 The date and time of opening of the Price Bids shall be communicated to the technically qualified Bidders in writing by e-mail or registered post/Speed Post; the Price Bids of only technically qualified Bidders shall be opened. A comparative statement shall be prepared detailing each price component in the bid and including all components of the Price Bid, as per **Clause 7.15.2**.

7.21 Preferred Bidder: The Bidder who submits the lowest Price Bid shall be the Preferred Bidder. The Preferred Bidder shall be issued the LoA. OMFED reserves the right to negotiate the price with the Preferred Bidder before issue of the LoA. The Preferred Bidder shall have to acknowledge and accept the LoA by returning a signed copy of the LoA within a period of 03 (Three) days of issue thereof, along with submission of the Performance Security, failing which the issued LoA may be cancelled and EMD of the Preferred Bidder shall be forfeited by OMFED.

7.22 Tie-Bidders:

In the event that 2 (two) or more technically qualified Bidders (the "Tie Bidders") have submitted the lowest identical Price Bids. OMFED shall hold an auction amongst such Tie Bidders. The auction shall be held at Corporate Office of OMFED and only the Tie Bidders shall be invited to attend the same, wherein they have to physically submit their revised Price Bids on their letterhead (with company rubber stamp) and in sealed covers. Hence the Authorized Signatory of the Tie Bidders are required to attend such auction. The revised Price Bid (the "Revised Price Bid") submitted by a Tie Bidder during the auction should be lower than Price Bid already submitted by it, else the revised Price Bid shall not be considered by OMFED for further evaluation. The Tie Bidder who offers the lowest revised Price Bid in such auction shall be declared to be Preferred Bidder and the lowest revised Price Bid received by OMFED during such auction shall be the L1 price. In the event that the Authorized Signatory of a Tie Bidder is not present during the auction or the Authorized Signatory of such Bidder does not or is unwilling to participate in such auction, the auction would be held amongst the remaining Tie Bidders and if there be only one remaining Tie Bidder, the latter will be declared as the Preferred Bidder, provided that the revised Price Bid submitted by such Bidder is lower than that its earlier submitted Price Bid; in such as case the revised Price Bid submitted by such Bidder shall be considered to be the L1 price. In case of a second round of tie between the revised Price Bids submitted by the Tie Bidders, the Bidder with the higher average annual turnover (to be determined by OMFED on the basis of the audited financial statements submitted by such Bidders as part of their Technical Bids) in the last 3 (three) financial years shall be declared as the Preferred Bidder and the L1 price shall be the revised Price Bid submitted by such Bidder during the auction.

7.23 Signing of Agreement:

Within 03 (Three) days of receipt of the signed copy of the LoA, along with the Performance Security, the Agreement shall be signed by the Preferred Bidder, failing which the Performance Security shall be forfeited and appropriated by OMFED. Upon signing of the Agreement, the Preferred Bidder shall be considered to be the "Successful Bidder". The pro-forma of the Agreement is provided in **Annexure-2A** hereof. Post signing of the Agreement, OMFED shall issue Service Order(s) to the Successful Bidder.

7.24 Performance Security: The formula for calculating the amount of the Performance Security is indicated in the Data Sheet. The Preferred Bidder shall submit the Performance Security at the Head Office, OMFED upon issue of LoA within a period of 15 (fifteen) days. Performance Security shall be in the form of a Bank Guarantee from any Nationalized/ Scheduled Bank invocable at their branch in Bhubaneswar as per the format given in **Annexure-7** or in the form of demand draft from a scheduled commercial bank and payable in Bhubaneswar, Odisha. Performance Security in the form of BG should be operable for invocation at any Nationalized/ Scheduled bank at Bhubaneswar.

The Performance Security will be valid for 12 (Twelve) months for each Contractual Year and the Performance Security shall be extended and adjusted for the next Contractual Year upon receiving the letter from OMFED to commence the subsequent Contractual Year's operation. The Performance Security shall be released on completion of the scope of services and shall be released after a period of 60 (sixty) days post completion of the scope of services including Warranty Period, as evidenced by issue of completion certificate by OMFED designated officer/ key contact for this contract.

8. Additional Information to Bidders

8.1 Pre-bid meeting:

8.1.1 A pre-bid meeting shall be organized by OMFED; the date and time of the pre-bid meeting is indicated in the Schedule for the Tender. Bidders wishing to attend the pre-bid meeting should inform OMFED by email (Refer Data Sheet), along with the names and email ids of the officials/ representatives of the Bidder who would be attending the meeting, at least 1 (one) working days before the pre-bid meeting. OMFED shall then send the invite for the pre-bid meeting to the email-ids that OMFED would be receiving.

8.1.2 However, attendance of the Bidders at the pre-bid meeting is not mandatory. A maximum of two officials/ representatives from each Bidder may attend the pre-bid meeting. All costs of the Bidder related to attending the pre-bid meeting shall be borne by the Bidder.

9. Additional Information on E-tendering process

9.1 The e-tendering process shall be held on the e-procurement portal of the Government of Odisha (www.tendersodisha.gov.in). All the steps involved starting from hosting of tenders till determination of the Selected Bidder shall be conducted online on the e-procurement portal.

9.2 The Bidder will have to accept unconditionally the online user portal agreement which contains the acceptance of all the terms and conditions including commercial and general terms and conditions and other conditions, if any, along with on-line undertaking in support of the authenticity of the declarations regarding the facts, figures, information and documents furnished by the Bidder on-line in order to become an eligible Bidder. No conditional bid shall be allowed / accepted.

9.3 The Bidder will have to give an undertaking online that if the information/ declaration/scanned documents furnished in support of the same in respect of eligibility criteria are found to be wrong or misleading at any stage, they will be liable to punitive action and this includes forfeiture of EMD and cancellation/ termination of contract/Agreement.

9.4 The Bidder will submit their Technical Bid and Price Bid on-line. The Bidders will have to upload a scanned copy of the Technical Bid in Cover-I; the Price Bid is to be submitted in Cover-II.

9.5 Procedure for bid submission and payment of Tender Paper Fee and EMD.

9.5.1 **Log on to e-procurement portal:** The Bidders have to log onto the e-procurement portal of the Government of Odisha (www.tendersodisha.gov.in) using their digital signature certificate and then search and then select the required active tender from the "Search Active Tender" option. Then the submit button can be clicked against the selected tender so that it comes to the "My Tenders" section.

9.5.2 **Uploading of the Technical Bid and the Price Bid:** The Bidders have to upload the required Technical Bid and the Price Bid, as mentioned in the tender document and in line with the Works Department office memorandum no.7885, dated 23 July 2013.

9.5.3 **Payment of Tender Paper Fee and EMD:** Tender Paper Fee and EMD shall be paid using a single banking transaction. The Bidders have to select and submit the bank name as available in the payment options. A Bidder shall make electronic payment using his/her internet banking enabled account with designated banks or their aggregator banks. The payment gateways of the designated banks (State Bank of India/ ICICI Bank, HDFC Bank) are integrated with the e-procurement portal. A Bidder having account in other banks can make payment using NEFT/RTGS facility of designated banks. Online NEFT/RTGS payment can be done using internet banking of the bank in which the Bidder holds his account, by adding the account number as mentioned in the challan as an interbank beneficiary. Only those Bidders who successfully remit their EMD on submission of bids would be eligible to participate on the tender/bid process. The Bidders with pending or failure payment status shall not be able to submit their bid. Tender Inviting Authority, State Procurement Cell, NIC and the designated Banks shall not be held responsible for such pendency or failure.

9.5.4 **Bid submission:** Only after receipt of intimation at the e-procurement portal regarding successful transaction by Bidder, the system will activate the 'Freeze Bid Submission' button to conclude the bid submission process.

9.5.5 System generated acknowledgement receipt for successful bid submission: System will generate an acknowledgement receipt for successful bid submission. The Bidder should make a note of 'Bid ID' generated in the acknowledgement receipt for tracking their bid

status.

9.5.6 Settlement of EMD on submission of bids: The Bank will remit the Earnest Money Deposit on cancellation of bids to respective Bidder's account as per direction received from Tender Inviting Authority through e-procurement system.

9.5.7 Forfeiture of EMDs: The forfeiture of EMD on submission of bid of defaulting Bidder may be occasioned for various reasons. In case the EMD Deposit on submission of bid is forfeited, the e-Procurement portal will direct the Bank to transfer the EMD value from the Pooling Account of SPC to the registered account of the Tender Inviting Authority, i.e. OMFED.

9.6 **Price Bid:** The price bid containing the bill of quantity will be in Excel format (or any other format) and will be uploaded by OMFED during tender creation. This will be downloaded by the Bidder and will be used to quote the Price Bid, inclusive of all taxes & duties etc. Thereafter, the Bidder will upload the same Excel file during bid submission in Cover-II. The L1 price will be decided for module as stipulated in the tender. The Price Bid of the Bidders will have no conditions. The Price Bid which is incomplete and not submitted as per instructions given shall be summarily rejected by OMFED without any further reference to the Bidder.

9.7 **Modification of bids:** Modification of the submitted bid shall be allowed online only before the Bid Due Date. A Bidder may modify and resubmit the bid online as many times as he may wish. Bidder may withdraw only once its Bid online within the end date of Bid submission.

9.8 **Opening of Technical Bids:** The Technical Bids shall be opened as per the schedule given in the Schedule of Tender. The Techno Commercial bids (Cover-I) will be decrypted on-line and will be opened by the designated bid openers of OMFED with their Digital Signature Certificates (DSC). The Technical Bids shall be opened as per the schedule, irrespective of the number of bids received. Even in case of receipt of single bid, the Technical Bid shall be opened for evaluation. In case no bids are received, the tender shall be automatically cancelled with approval of the competent authority of OMFED.

9.9 Evaluation of Technical Bids: The Technical Bids shall be evaluated in terms of **Clause 7.19**. If required, OMFED may ask Bidders to provide clarifications on their bid or provide shortfall documents within a period of 3 (three) working days. The Bidders will get this information on their personalized dash board under "Upload shortfall document/information" link. However, no changes in the Price Bid shall be sought, offered or permitted, nor shall the documents sought be related to the EMD or the Tender Paper Fee. No modification of the bid or any form of communication with OMFED or submission of any additional documents which are not specifically asked for by OMFED, will be allowed and even if submitted, they will not be considered by OMFED. Additionally, information shall also be sent by system generated e-mail and SMS, but it will be the Bidder's responsibility to check the updated status/information on their personalized dash board at least once daily after opening of bid. No separate communication will be required in this regard. Non-receipt of email and SMS will not be accepted as a reason for non-submission of documents within prescribed time. The Bidder shall submit the requisite clarifications and the requested documents and in the Upload Shortfall

document section of the e-procurement portal within the specified period and no additional time will be allowed for submission of the clarifications/ documents. In case of any failure of the Bidder to submit the requisite documents within the allowed timeframe, OMFED shall proceed to evaluate its Technical Bid without any further reference to the Bidder.

9.10 Based on the evaluation of the Technical Bids, the list of technically qualified Bidders shall be prepared and the same shall be uploaded, along with the date and time of opening of Price bid in the portal and such Bidders shall also be informed through system generated e-mail and SMS alert. The Price Bid of such shortlisted Bidders shall be decrypted and opened on the scheduled date and time by the designated bid openers of OMFED with their Digital Signature Certificates. The Bidders may view the price bid opening online remotely on their personalized dash board under the link "Bid Opening (Live)" and can see the Price Bid /BOQ submitted by all shortlisted Bidders.

9.11 A comparative statement of the Price Bids shall be generated by the e-procurement system. The same shall be downloaded and will be signed by the officers of OMFED opening the Price Bids and submitted to the competent authority of OMFED for approval and further necessary action. The comparative statement shall also be viewable to the participating Bidders whose Price Bids were opened. In case of tie bids, the same shall be dealt with in terms of **Clause 7.22**.

9.12 Upon approval and completion of the due process of OMFED, the Preferred Bidder shall be issued the LoA in terms of **Clause 7.21**. The LoA shall be sent through registered/ speed post to the office address of the Preferred Bidder; a scanned copy of the Agreement/Service Order shall also be uploaded on the e-procurement portal.

Annexure 1: General Conditions of Contract-Services

1. Definitions

In the interpretation of the Contract and the general and special conditions governing it, unless the context otherwise requires:

1.1 "Contract Price" or "Contract Value" shall mean the price payable to the Service Provider under the Service Order / Agreement for the full and proper performance of his contractual obligations;

1.2 "Service Order" or "Contract" or "Agreement" shall mean the Service Order / Agreement and all attached exhibits and documents referred to therein and all terms and conditions thereof together with any subsequent modifications thereto;

1.3 "Site" shall mean the place or places named in the Service Order / Agreement or such other place or places at which any work has to be carried out as may be approved by OMFED;

1.4 "Service Provider" or "Contractor" shall mean a firm or company with whom the Service Order / Agreement is placed and shall be deemed to include the supplier in successors (approved by OMFED) representatives, heirs, executors, administrators and permitted assignee as the case may be;

1.5 "Services" means the services specified in the Service Order which the Service Provider has agreed to supply under Service Order / Agreement;

2. Scope of Services

2.1 Scope of Services shall be as defined in the Special Conditions of Contract and Annexure thereto.

3. Instructions, Direction & Correspondence

3.1 All instructions and orders to Service Provider shall, excepting what is herein provided, be given by OMFED.

3.2 All the work shall be carried out under the direction of and to the satisfaction of OMFED.

3.3 All communications including technical/commercial clarifications and/or comments shall be addressed to OMFED shall always bear reference to the Service Order / Agreement.

3.4 Invoices for payment against Service Order / Agreement shall be addressed to OMFED.

3.5 The Service Order / Agreement number shall be shown on all challans / invoices, communications, packing lists, containers and bills of lading (as applicable), etc.

4. Service Order / Agreement Obligations

4.1 If after award of the LoA, the Service Provider does not acknowledge the receipt of award or fails to furnish the Performance Security within the prescribed time limit (as the case maybe), OMFED reserves the right to cancel the LoA and forfeit

the EMD.

4.2 Once a Service Order / Agreement is accepted and confirmed and signed, the terms and conditions contained therein shall take precedence over the Service Provider's bid and all previous correspondence.

4.3 The Service Order/ Agreement shall, in all respects, deemed to be and shall construe and operate as an Indian Contract in conformity with the Indian Laws.

5. Modification in Service Order / Agreement

5.1 All modifications leading to changes in the Service Order / Agreement with respect to technical and/or commercial aspects including terms of delivery of services, shall be considered valid only when accepted in writing by OMFED by issuing amendment to the Service Order / Agreement. Issuance of acceptance or otherwise in such cases shall not be any ground for extension of agreed delivery date and also shall not affect the performance of Service Order / Agreement in any manner except to the extent mutually agreed through a modification of Service Order / Agreement.

5.2 OMFED shall not be bound by any printed conditions or provisions in the Service Provider's Bid Forms or acknowledgment of Service Order / Agreement, invoices and other documents which purport to impose any conditions at variance with or supplemental to Service Order / Agreement.

6. Use of Service Order / Agreement Documents & Information

6.1 The Service Provider shall not, without OMFED's prior written consent, disclose any approved plan, drawing, pattern, sample or information furnished by or on behalf of OMFED in connection therewith, to any person other than a person employed by the Service Provider in the performance of the Service Order / Agreement. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purpose of such performance.

6.2 The Service Provider shall not, without OMFED's prior written consent, make use of any document or information enumerated in above Clause 6.1 except for purpose of performing the Service Order / Agreement.

7. Patent Rights, Liability & Compliance of Regulations

7.1 Service Provider hereby warrants that the use of the services delivered hereunder will not infringe claims of any patent covering such service and Service Provider agrees to be responsible for and to defend at his sole expense all suits and proceedings against OMFED based on any such alleged patent infringement and to pay all costs, expenses and damages which OMFED may have to pay or incur by reason of any such suit or proceedings.

7.2 The Service Provider shall indemnify OMFED against all third-party claims of infringement of patent, trade mark or industrial design rights arising from the services delivered by the Service Provider.

7.3 Service Provider shall be responsible for compliance with all requirements under the laws and shall protect and indemnify completely OMFED from any claims/penalties arising out of any infringements.

8. Performance Security

8.1 The Service Provider shall furnish Performance Security as per the terms and conditions provided in the Tender document.

8.2 The Performance Security shall be for due and faithful performance during the period of execution of the services and is liable for forfeiture in the following cases:

- If the successful Bidder fails to undertake the work after issuance of LoA, or
- If the Service Provider abandons the work before its completion or during its extended period, or
- If the work performed by the Service Provider is not as per the Agreement, or
- On breach of Service Order / Agreement by the Service Provider.

8.3 The proceeds of Performance Security shall be appropriated by OMFED as compensation for any loss resulting from the Service Provider's failure to complete his obligations under the Service Order / Agreement without prejudice to any of the rights or remedies OMFED may be entitled to as per terms and conditions of Service Order / Agreement.

8.4 Performance Security shall be extended by the Service Provider in the event of delay in completion of work, as defined in the Service Order / Agreement for any reason whatsoever. OMFED's claim period shall remain valid for twelve months after the expiry of the guarantee/warrantee/Defect Liability Period or till the satisfactory performance of the objectives of the Service Order / Agreement, whichever is later.

8.5 For the avoidance of doubt, it is hereby clarified, that the Performance Security shall not carry any interest.

9. Delivery of Services

9.1 Delivery of the Services shall be made by the Service Provider in accordance with terms specified in the Special Conditions of Contract.

9.2 The delivery terms are binding and essential and consequently, no delay is allowed without the written approval of OMFED. Any request concerning delay will be null and void unless accepted by OMFED.

10. Terms of Payment

10.1 Details about the method of payment, payment terms, billings, place of payment, etc. under this Service Order / Agreement shall be specified in the Special Conditions of Contract.

10.2 All payments shall be made in INR only and shall be made directly to the bank account of the Service Provider.

10.3 No advance shall be paid and no letter of credit shall be issued.

10.4 Payment shall be released within 30 (thirty) days after receipt of relevant documents complete in all respects and successful Completion Certificate issued by under section of OMFED.

10.5 No interest charges for some reasonable delay in payments, if any, shall be payable by OMFED.

10.6 Defective bills shall be returned to the Service Provider within 7 (seven) working days. No payment shall be made on defective/incomplete bills.

11. Subcontracting /out-sourcing/ sub-letting/ Assignment

11.1 The Service Provider is not allowed to subcontract, outsource, sub-let or assign the contract and scope of services, either partly or wholly, without the written approval of the designated official or Nodal Officer from OMFED side for the services for which such subletting is sought. However, OMFED management reserves the full right to refuse any such approval to the Service Provider without being bound to provide any reason or rationale for such decision. Provided, nevertheless, that any such consent shall not relieve the Service Provider from any obligation, duty or responsibility under the Service Order / Agreement.

12. Cancellation of Service Order / Agreement

12.1 If the Service Provider fails to fulfil the terms and conditions of the Service Order / Agreement which are spelt out in the Tender Document, OMFED shall have the right to terminate the Service Order / Agreement and award the total or balance work (if any) to any other Service Provider at the risk and cost of the said Service Provider after giving 30 days' notice to the Service Provider as to why the said work shall not be awarded to another entity at his risk and cost. Further the Service Order/Agreement could be terminated by OMFED if:

i) There is a force-majeure situation,
ii) Service Provider has given false declaration or document including affidavit,
iii) There is conflict of interest between OMFED& Service Provider during the Service Order / Agreement execution,
iv) The Service Provider defaults in proceeding with the work as per the milestones and/or in complying with any of the terms and conditions, stipulated in the Service Order / Agreement,
v) The Service Provider or firm or any of the partner represented by the Service Provider, in the subject Service Order / Agreement is adjudged as Insolvent by the concerned authority and further if the Service Provider has been wound up and dissolved,
vi) The Service Provider assigns/transfers/sub-lets the entire work or a portion thereof without the approval of the Competent Authority,
vii) The Service Provider offers to give or agrees to give gift or any other consideration tangible or intangible, as inducement or reward for seeking or offering benefits in the Service Order / Agreement as the case may be,
viii) A court order or an order of a competent statutory forum is received in respect of the Service under consideration of the Service Order / Agreement.

Termination of the agreement shall not relieve the Service Provider of any obligations which expressly or by necessary implication survives termination. Except as otherwise provided in any provisions of the agreement expressly limiting the liability of the Service Provider, shall not relieve the Service Provider of any obligations or liability for loss or damage to OMFED arising out of or caused by acts or omissions of the Service Provider prior to the effective date of

termination or arising out of such termination. Even if Service Order / Agreement is terminated/abandoned prematurely, OMFED reserves the right to deduct/impose penalties and remain indemnified, till such time all or any such claims are suitably addressed. OMFED reserves the right to appropriate the Performance Security, as a genuine pre-estimated damage suffered by OMFED for the non-performance by the Service Provider. OMFED may also impose further penalties on the Service Provider such as holidaying/banning/blacklisting for a specific period of time. In all such cases, the decision of OMFED shall be final. This notice shall be in accordance with above **Clause 12.1**.

13. Right to risk for procurement / rendering of services

If the Service Provider fails to fulfill the terms and conditions of the Service Order / Agreement, OMFED shall have the right to procure the services from any other party for the execution/ completion of the scope of services under the Service Order / Agreement and recover from the Service Provider all charges/expenses/losses/damages which may be suffered by OMFED, at the risk and cost of the Service Provider, after giving 15 (fifteen) days of notice to the Service Provider. This will be without prejudice to the rights of OMFED for any other action including termination of the Service Order/ Agreement.

14. Force Majeure

14.1 "Force Majeure Event" means any event or circumstances or combination of events or circumstances which:

A. Are beyond the reasonable control of the Party affected by such event (the Affected Party); and cannot by exercise of reasonable diligence, reasonable precautions and reasonable alternative measures (where sufficient time to adopt such precautions or alternative measures before the occurrence of such event or circumstances is available), be prevented or caused to be prevented;

B. Materially and adversely affects such Party's performance of its duties or obligations or enjoyment of its rights under this Service Order / Agreement.

14.2 As soon as practicable and in any case within 7 (seven) days from the date of occurrence of a Force Majeure Event or the date of knowledge thereof, the Affected Party shall notify the other Party of the same, setting out the details of the Force Majeure Event.

14.3 If the Affected Party is rendered wholly or partially incapable of performing any of its obligations under this Service Order / Agreement because of a Force Majeure Event, it shall be excused from performance of such obligations to the extent it is unable to perform the same on account of such Force Majeure Event.

14.4 If a Force Majeure Event described above, in the reasonable judgment of the Parties, is likely to continue beyond a period of 6 (six) months or any other period as stipulated in the Bid document, the parties may mutually decide to terminate the Service Order /Agreement or continue the Service Order / Agreement on mutually agreed revised terms.

15. Dispute Resolution

15.1 Any dispute, difference or controversy of whatever nature howsoever arising under, or out of, or in relation, to this tender or the Service Order / Agreement (including its interpretation) between OMFED and the Service Provider, and so notified in writing by either party to the other party shall, in the first instance, be attempted to be resolved amicably and the parties agree to use their best efforts

for resolving all disputes arising under or in respect of this tender promptly, equitably and in good faith. In the event of any dispute between the parties, it is agreed that a discussion shall be held between the Service Provider and OMFED within 7 (seven) days from the date of reference to discuss and attempt to amicably resolve the dispute. If such meeting does not take place within the 7 (seven) days period or the dispute is not amicably settled within 15 (fifteen) days of the meeting, the dispute, if referred to, shall be decided by the Civil Court of competent jurisdiction at Bhubaneswar only. There shall be no arbitration between the Parties. The provisions of Arbitration & Conciliation Act, 1996 as amended from time to time, shall have no application to the present work.

15.2 Governing law and jurisdiction: This Service Order / Agreement shall be construed and interpreted in accordance with and governed by the laws of State and Central Government in force in India. The Courts at Bhubaneswar alone shall have exclusive jurisdiction over all matters arising out of or relating to this Service Order / Agreement.

16. Governing Language

The Service Order / Agreement shall be written in English language as specified by OMFED in the Instruction to Bidders. All literature, correspondence and other documents pertaining to the Service Order / Agreement which are exchanged by the parties shall be written in English language. Printed literature in other language shall only be considered, if it is accompanied by an English translation. For the purposes of interpretation, English translation shall govern and be binding on all parties.

17. Notices

Any notice given by one party to the other pursuant to the Service Order / Agreement shall be sent in writing or by email. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

18. Permits & Certificates

18.1 Service Provider shall procure, at his expense, all necessary permits, certificates and licenses required by virtue of all applicable laws, regulations, ordinances and other rules in effect at the place where any of the work is to be performed, and Service Provider further agrees to hold OMFED harmless from liability or penalty which might be imposed by reason of any asserted or established violation of such laws, regulations, ordinances or other rules.

19. General

19.1 The Service Provider shall be deemed to have carefully examined all Service Order / Agreement documents to its entire satisfaction. Any lack of information shall not in any way relieve the Service Provider of his responsibility to fulfill his obligation under the Service Order / Agreement documents.

19.2 The General Conditions of Contract (GCC)-Services shall apply to the extent that they are not superseded by provisions of other parts of the Special Conditions of Contract.

19.3 **Losses due to non-compliance of Instructions**

Losses or damages occurring to OMFED owing to the Service Provider's failure to adhere to any of the instructions given by OMFED in connection with the contract execution shall be recoverable from the Service Provider.

19.4 **Recovery of sums due**

All costs, damages or expenses which OMFED may have paid, for which under the

Service Order / Agreement, the Service Provider is liable, may be recovered by OMFED (he is hereby irrevocably authorized to do so) from any money due to or becoming due to the Service Provider under this Service Order / Agreement or other Service Orders / Agreements and/or may be recovered by action at law or otherwise. If the same due to the Service Provider be not sufficient to recover the recoverable amount, the Service Provider shall pay to OMFED, on demand, the balance amount.

20. Liability and Indemnity

20.1 Service Provider shall indemnify, defend and hold OMFED harmless against:

a. any and all third party claims, actions, suits or proceedings against OMFED, for any loss of or damage to property of such third party, or death or injury to such third party, arising out of breach by the Service Provider of any of its obligations under the Service Order / Agreement, except to the extent that any such claim, action, suit or proceeding has arisen due to a negligent actor omission, breach of the Service Order / Agreement, or breach of statutory duty on the part of OMFED, its suppliers and Service Providers, employees, servants or agents; and

b. any and all losses, damages, costs, and expenses including legal costs, fines, penalties and interest actually suffered or incurred by OMFED from third party claims arising by reason of breach by the Service Provider of any of its obligations under this Service Order / Agreement, except to the extent that any such losses, damages, cost & expenses including legal costs, fines, penalties and interest (together to constitute "Indemnifiable Losses") have arisen due to negligent act or omission breach of the Service Order / Agreement, or breach of statutory duty on the part of OMFED, its suppliers or Service Providers, employees, servants or agents or any of the representations; and

c. To the extent of the value of free issue materials to be issued till such time the entire Service Order / Agreement is executed and proper account for the free issue materials is rendered and the left over / surplus and scrap items are returned to OMFED. The Service Provider shall not utilize OMFED's free issue materials for any job other than the one contracted out in this case and also not indulge in any act, commission or negligence which will cause / result in any loss/damage to OMFED and in which case, the Service Provider shall be liable to OMFED to pay compensation to the full extent of damage / loss and undertake to pay the same.

20.2 OMFED remains indemnified (even if the Service Order / Agreement ends pre-maturely) towards all or any obligations due to OMFED by the Service Provider and shall continue to remain in force till such time all or any such claims are suitably addressed.

21. Publicity & Advertising

Service Provider shall not without the written permission of OMFED make a reference to OMFED or any Company affiliated with OMFED or to the destination or the description of goods or services supplied under the Service Order / Agreement in any publication, publicity or advertising media.

22. Blacklisting

Blacklisting of a business concern/entity or supplier may be resorted to in following cases: -

i) If the Proprietor or Partner or Director of the business concern/entity is convicted by a Court of Law, following prosecution under the normal process of Law for an offence involving moral turpitude in relations to business dealings;

ii) If security consideration of the state i.e. any action that jeopardize the security of the State.

iii) If there is justification for believing that the Proprietor or Partner or Director of the Concern/entity has been guilty of malpractices such as bribery, corruption, cheating, fraud and tender fixing etc.

iv) If the business concern/entity refuses / fails to return OMFED's dues without adequate cause;

v) If the business concern/entity is blacklisted by any Department of the Central Government / State Government/Central PSU/State PSU.

vi) If the business concern/entity is a concern/entity evader of Central / State taxes / duties for which OMFED has received notice from the concerned department of Central / State Govt.

vii) If violation of important conditions of contract/agreement.

viii) If submission of false/fabricated/forged documents for consideration of a tender

23. Statutory and Legal requirements

23.1 The Service Provider shall comply with all the statutory and legal requirements and requirements for obtaining license under the Contract Labour (Regulation and Abolition) Act 1970 and shall bear all necessary expenses in this regard.

23.2 The Service Provider shall abide by the applicable statutory provisions on minimum wages, payment of wages, EPF, ESI, gratuity, retrenchment, leave and leave encashment, health care, uniform and compensation to its employees and workmen.

23.3 The Service Provider shall not take any action in relation to handling of its personnel which may adversely affect the existing labour relations of OMFED. The Service Provider has to maintain close liaison and cordial relations with the local people and the unions.

24. Safety

24.1 OMFED may from time to time audit the safety practices employed by the Service Provider and the Service Provider shall comply with the recommendations/ directions made by OMFED as a result of such audit.

24.2 During the course of the contract period, if any accident occurs whether major or minor in which the Service Provider or its employees are involved or are responsible, the Service Provider shall immediately inform OMFED without any delay.

24.3 The Service Provider shall indemnify OMFED from any liability falling on OMFED due to any accident, whether minor or major, or by any act of commission/omission by the Service Provider or by its representatives or by its employees. If OMFED is made liable for any such claim by the court of law or any other authority, the same shall be reimbursed to OMFED by the Service Provider as if OMFED has paid on their behalf. The same shall be adjusted from the invoices payable by OMFED to the Service Provider, if not paid within a period of 30 (thirty) days of such payment being made by OMFED.

Annexure 2: Special Conditions of Contract

1. General

These Special Conditions of Contract delete, amend or add to the clauses in the General Conditions of Contract. In the event of an inconsistency, these Special Conditions of Contract shall supersede or take precedence over the General Conditions of Contract to the extent of that inconsistency.

2. Scope of work, service requirements including technical parameters

2.1 Background

The Orissa State Cooperative Milk Producers' Federation Limited (OMFED) is the apex-level Dairy Cooperative Society, registered under the Cooperative Society Act of 1962. It was established to bridge the gap between rural milk producers and urban consumers, fostering growth with an entrepreneurial spirit.

OMFED's core activities include promotion, production, procurement, processing, and marketing of milk and milk products, as well as providing subsidized cattle feed, thereby supporting the economic growth of the rural farming community in Odisha. With a large workforce operating across various locations, OMFED is now aiming to implement a Unified Command & Control (UCC) Platform-based CCTV Surveillance system at Arilo Dairy to address pressing security concerns that are affecting daily operations. The proposed UCC platform-based surveillance system aims to enhance the security framework at Arilo Dairy by enabling centralized monitoring and streamlined security processes. This initiative is intended to create a more secure environment, ensuring the safety and smooth operation of daily activities.

OMFED is inviting vendors to provide a reliable and robust solution that aligns with the functional and technical specifications outlined in the Tender Document. The chosen vendor will be responsible for the supply, implementation, and ongoing maintenance of the system. The project is expected to be executed within the stipulated timeline mentioned in the subsequent sections. Additionally, the vendor must provide training for OMFED's staff on system usage and maintenance. Post-implementation support and maintenance services will be required for a period of five years from the system's Go-live date.

2.2 Implementation Scope

This Scope of Work outlines the design, procurement, installation, integration, testing, and commissioning of a **Unified Command & Control (UCC) Platform-based CCTV Security Surveillance System** for the Arilo Dairy Plant, Cuttack, operated by OMFED. The system will include advanced integrated features such as access control, Automatic License Plate Recognition (ANPR/ALPR), perimeter intrusion detection, and AI/ML-based video analytics. It is aimed at enhancing security, monitoring employee behaviour, and ensuring operational efficiency.

1. **Unified Command & Control (UCC) Platform Implementation**
    - **Platform Overview**: Centralized open software capable of managing and integrating all components of the CCTV Security Surveillance System, Access Control, ANPR/ALPR, and AI/ML analytics from a **single platform** for efficient management and operation.
    - **Key Features**:

- Real-time monitoring of all connected cameras and sensors.
- Centralized dashboard for live video feeds, alerts, and event reporting.
- Role-based access control for different user levels (operators, supervisors, administrators).
- Incident management and report generation.
- Scalability to accommodate future expansion.

2. **High-Resolution EDGE AI CCTV System**
   - **Fixed and PTZ Cameras**:
     - **Coverage**: Strategic installation at key points such as entrances/exits, production areas, storage zones, employee break areas, and perimeter boundaries.
     - **High-Resolution Imaging**: Minimum 4K cameras for clear imaging in both day and night conditions (IR/night vision).
     - **PTZ Cameras**: For real-time perimeter surveillance and tracking of intrusions with 360-degree coverage and zoom capabilities.
     - **Recording and Archiving**: Continuous video recording with at least 90 days of storage, and options for long-term archival.
   - Ensure the cameras are capable of **24x7 surveillance** and integration with the UCC platform for centralized management.

3. **Control Room Setup**
   - Design and implement a **state-of-the-art Control Room** equipped with a **video wall** to view live and recorded footage from the entire system.
   - Provide a **power backup solution** to ensure uninterrupted operation of the control room during power outages.

4. **Access Control System:**
   - **Entry/Exit Points**: RFID, Biometric, or Smart Card-based access control at all employee and visitor entry points.
   - **Employee Attendance Management**: Integration with the existing attendance system to ensure automated employee check-ins/check-outs.
   - **Alarm Triggers**: In case of unauthorized access attempts, the system will trigger alarms to the command center.
   - Integrate the access control system into the UCC platform for **centralized monitoring** and control.

5. **Automatic Number/License Plate Recognition (ANPR/ALPR) System:**
   - **Vehicle Monitoring**: Installation of ANPR/ALPR cameras for automatic capture of license plate details of all vehicles at entry and exit points and weigh bridges for errorless integration into respective applications.
   - **Vehicle Movement Tracking**: Real-time tracking of vehicle movements within the plant premises.
   - **Whitelisting and Blacklisting**: Authorized vehicles can be pre-registered, and any unauthorized vehicle entries will trigger alerts.
   - **Event Logs**: Storing vehicle entry/exit records for review and reporting purposes.
   - Integrate the ANPR/ALPR system into the UCC platform.

6. **Perimeter Intrusion Detection:**
   - **PTZ Cameras**: Installed along the perimeter of the dairy plant to detect unauthorized access or suspicious activity.
   - **Motion Detection & Tracking**: Cameras equipped with motion sensors to trigger alerts in the command center upon detecting movement near the perimeter.

- **Automated Incident Management**: Any detected intrusion is automatically tracked by PTZ cameras, and operators are alerted to take appropriate action.

7. **Public Announcement (PA) System**
   - Install an **IP-based Public Announcement System** at strategic points in the plant.
   - Integrate the PA system into the UCC platform, allowing announcements to be made from the control room.
8. **Variable Digital Display Boards**
   - Integrate **variable digital display boards** around the plant into the UCC platform, allowing real-time communication with staff and visitors.
9. **SIP Communications and Mobile Camera App**
   - Provide **SIP-based communication systems** for easy communication between staff and the control room.
   - Develop and integrate a **mobile camera app** to stream footage from mobile devices directly into the UCC platform for real-time monitoring.
10. **Integration of Existing CCTV Feeds**
    - Securely integrate **existing CCTV cameras** into the UCC platform, ensuring data protection from **cyber threats** and preventing **data leakage**.
11. **Incident Management Module**
    - Implement an **incident management module** within the UCC platform for prompt action during emergencies such as:
      - Accidents
      - Unauthorized access
      - Fires or smoke
      - Unruly behavior or fights
    - Enable notifications, alarms, and alerts to be generated and displayed on the **dashboard** for swift response by field responders.
12. **Advanced AI and ML-Based Video Analytics**
    - Provide an **AI/ML-based video analytics platform** integrated with the CCTV system for:
      - **Video synopsis** and **quick search** capabilities.
      - **Real-time health monitoring** of cameras, sensors, and other IoT devices.
    - **Hygiene Compliance**: Real-time monitoring of employees for compliance with hygiene regulations, such as handwashing, mask usage, and sanitation in designated areas.
    - **PPE Kit Compliance**: AI-based detection of Personal Protective Equipment (PPE) such as helmets, gloves, and vests. The system generates alerts for non-compliance.
    - **Unruly Behavior Detection**:
      - **Behavioral Analysis**: AI-based algorithms to detect suspicious behaviour patterns such as unauthorized gatherings, aggressive behaviour, or unsafe actions.
      - **Real-Time Alerts**: Automated notifications to the security command center for immediate investigation and action.

- **Reporting & Analytics**: Generation of reports on hygiene and PPE compliance, attendance irregularities, and recorded incidents of unruly behaviour.

13. Third-Party Application Integration

- Provide integration support for **third-party applications**, including:
    - **SAP/ERP systems**
    - **Logistic management systems**
    - **Map services**
    - **Social media platforms**
    - **Mobile applications**
- Facilitate data correlation for **quick and informed decision-making**.

14. Future Expansion Capabilities

- The UCC platform must be **scalable** and support future expansion, including:
    - **Vehicle tracking systems** for milk pickup and product distribution.
    - **Automation systems** for milk unloading and finished product loading.
    - **RFID-based crate monitoring** systems.
    - Detection and prevention of **pilferage** across the product life cycle.

15. Unlimited Camera and Server Connectivity

- Ensure the UCC platform is capable of supporting **unlimited cameras, recording servers, and client connections** across multiple sites.
- All components should be easily accessible through a **centralized management server**.

16. Mobile App and Website Access

- Enable **remote access** to live and recorded footage through a **mobile app** and **website** interface for authorized users.

17. Video Recording and Storage

- Ensure all cameras record footage **24x7** in HD resolution or better for a minimum of **60 days**, with the option to extend storage to **90 days** or more.

18. Simultaneous Viewing and Control

- Facilitate the **simultaneous viewing** of live and recorded footage by multiple authorized users without degrading the video quality.
- Enable control of all cameras and subsystems from the UCC platform.

19. Centralized Command and Control Room

- Ensure all surveillance feeds from different locations are sent to the **Centralized Command and Control Room**.
- The control room will include a **video wall** displaying a specified number of camera feeds simultaneously.

20. Installation & Commissioning:

- **Site Survey**: A comprehensive site survey must be conducted to identify camera locations, access points, and perimeter zones.
- **Installation**: All cameras, access control devices, and ANPR/ALPR systems must be installed in accordance with the approved site plan. Cabling, network setup, and power backup systems must also be installed to ensure uninterrupted operation.

- **Testing**: Comprehensive system testing including camera functionality, access control integration, ANPR/ALPR accuracy, perimeter intrusion detection, and AI/ML analytics performance.
- **Commissioning**: Once testing is complete, the system will be commissioned for use and handed over to the plant security team.

21. Training & Documentation:

- **Training**: Provide training to the plant security personnel and system operators on how to use the UCC platform, monitor video feeds, manage access control, and respond to incidents.
- **User Manuals**: Detailed user manuals and operational guides for system components must be provided.
- **Maintenance Guides**: Documentation on system maintenance, troubleshooting, and periodic testing schedules.

22. Maintenance & Support:

- Provide **Operation and Maintenance (O&M)** services for the entire system for **five (5) years** from the date of commissioning.
- The O&M services will include regular updates, troubleshooting, and system optimization.
- **24/7 Support**: Availability of 24/7 remote technical support and on-site support as needed.

23. Deliverables:

- Fully functional and integrated Unified Command & Control-based CCTV Security Surveillance System.
- AI/ML-powered video analytics for Quick Search, Video Synopsis, Health monitoring of devices, monitoring employee behaviour, hygiene, and PPE compliance.
- Automated vehicle monitoring with ANPR/ALPR for entry, exit, and movement tracking.
- Perimeter intrusion detection system with PTZ cameras.
- Access control system integrated with the UCC platform.

This detailed Scope of Work outlines the essential requirements for a comprehensive, future-proof, and scalable **UCC Platform-based CCTV Security Surveillance System** for the Arilo Dairy Plant of OMFED. The solution will enhance security, operational efficiency, and safety within the plant premises while integrating state-of-the-art technologies to meet current and future demands.

2.3 Technical Specifications

1) EDGE BASED AI (ARTIFICAL INTELLIGENT) 5 MP BULLET CAMERA

Edge Based AI Bullet Camera - 5MP Camera			
Sl. No	**Parameter**	**Technical Specification**	**Compliance (Yes/No)**
1	Type	Bullet Camera	
2	Image Sensor	1/2.8" Progressive CMOS with deep learning feature or better	
3	Resolution	2560x1920 (5MP) or better	
4	Lens	f = 2.7~13.5 mm, P-iris, Motorized, Vari-focal, Remote Focus,F1.83(W) ~ F3.32(T),100.1° ~ 29.9° (Horizontal)	
5	Shutter Time	1/5 sec. to 1/30,000 sec. or better	
6	WDR	120dB or better	
7	Removable IR-cut Filter for Day/Night Settings	Yes with Supreme Night Visibility	
8	S/N Ratio	50 db or better	
9	IR Illuminators	Built-in IR illuminators, up to 50 meters or better	
10	Minimum Illumination	0.04 lux @ F1.4(Color)	
		<0.005 lux @ F1.4 (B/W)	
		0 lux with IR illumination on	
11	Video Frame Rate	30 fps @ 2560X1920 ,30 fps @ 2560X1440 ,60 fps @ 1920x1080 or better	
12	Video Streams	3 simultaneous streams (Up to 8 configurable profiles) or better	
13	On-board Storage	Seamless Recording to MicroSD/SDHC/SDXC card slot. The Camera should be support upto 1 TB SD Card class 10 and recording to network-attached storage (NAS). 512GB SD Card class need to supplied at time of bidding	
14	Video Streaming	Adjustable resolution, quality and bit rate control, Smart Stream III for bandwidth optimization	
15	Image Settings	video title and time stamp overlay, video orientation, anti-overexposure, white balance, brightness, contrast, saturation, sharpness, gamma curve, defog, 3DNR;Pixel calculator , BLC, HLC, Exposure level, iris adjustment, exposure time, gain control, iris mode , Privacy mask, Scheduled profile settings, AI-powered Image Enhancement	
16	Audio Capability	Two-way Audio (full duplex)	
17	Audio Compression	G.711, G.726	
18	Audio Interface	External microphone input	
		External line output	
19	Unicast	Upto 10 Live users or better	
20	Protocols	802.1X, ARP, Bonjour, CIFS/SMB, DDNS, DHCP, DNS, FTP/SFTP, HTTP/HTTPS, ICMP,	

		IGMPv3, IPv4, IPv6, NTP, PPPoE, QoS (CoS/DSCP), RTSP/RTP/RTCP, SMTP, SNMP, SSL, TCP/IP, TLS 1.2/1.3, UDP, UPnP	
21	Security	Access list, Account block , Audit log, Configurable password strength protection, CSRF protection, Digest authentication, HTTPS , IEEE 802.1x, Secure boot, Session timeout, Signed firmware, Brute force attack event, Cyberattack event, Quarantine event , User access log, User account management	
22	Interface	10 Base-T/100 Base-TX/1000 Base-T Ethernet (RJ-45)	
23	ONVIF	Profiles T, G & S Supported and available on onvif website. Camera OEM should be full membership of ONVIF and it is available on onvif website	
24	RAM/Flash	DDR5 2GB /eMMC 8 GB	
25	Cybersecurity Chipset	Embedded in Camera	
26	Smart Motion Detection	people detection, vehicle detection, time filter, video motion detection,	
27	Edge based Analytics	Intrusion detection, loitering detection, line crossing detection, unattended object detection, missing object detection, face detection, crowd detection, running detection, Object Detection, Object Attribute Extraction, Object Research Extraction, Object	
28	Alarm Triggers	Audio detection, camera tampering detection, brute force attack event, cyberattack event, quarantine event, digital input, manual trigger, motion detection, periodical trigger, recording notification, SD card life expectancy, shock detection	
29	Alarm Events	Event notification via audio clip, camera link, digital output, email, HTTP, FTP/SFTP, NAS server, SD card	
		File upload via email, HTTP, FTP/SFTP, NAS server, SD card	
30	IP Connectors	RJ-45 cable connector for 10/100/1000Mbps Network/PoE connection	
		Audio input	
		Audio output	
		AC 24V power input/DC 12V power input	
		Digital input *2	
		Digital output *1	
31	Power Input	DC 12V, IEEE 802.3af PoE Class 0 (Dual Power supported)	
32	Power Consumption	PoE: Max. 12W,DC 16V: Max. 9 W,AC 24V: Max.11	
33	Operating Temperature & Humidity	Starting Temperature:	
		-30°C ~ 60°C (-22°F ~ 140°F)	
		Working Temperature:	
		-40°C ~ 60°C (-40°F ~ 140°F) (IR off)	

		-40°C ~ 50°C (-40°F ~ 122°F) (IR on),98% RH (non-condensing) or better	
34	Safety Certifications for Camera	EMC: CE (EN 55032/EN 55035 Class A, EN 50121-4), FCC (FCC Part 15 Subpart B Class A), VCCI (VCCICISPR 32 Class A),ICES-003 Issue 7 ; Safety: UL (UL 62368-1), CB /IEC/EN 62368-1, CB/IEC/ EN 60950-22, CB/IEC/EN 62471), LVD, (EN 62368-1), IK10 (IEC 62262), IP66/67 (IEC 60529), NEMA (NEMA 250 Type 4X), IEC 60068-2-11, BIS	
35	NDAA Compliant & Non HI silicon SOC	Yes	
36	MTBF	More than 300,000 hrs	
37	OEM Declaration	Any of the proposed in cameras should not contain any "HI Silicon make chipset / SoC / Sensor / Any other Low end chip manufacturer with Security issues /parts. Camera OEM need to submit declaration on letter head regarding quoted model specific sensor and SoC details (Make, Model etc.)	
38	End to End Encryption	The camera and software should be open platform integrated with other makes at SDK level. However they should have end to end encryption.	
39	OEM Declaration	The MAC address of all cameras should not be registered in the name of any OEM / company / entity sharing land border with India until unless specifically allowed by the Government of India and it should be registered in name of camera OEM. The Equipment supplied should not be manufactured by an entity in which the majority shareholding of the entity is from sharing land border with India. OEM Should not have used any component from neighboring countries and needs to mentioned country of origin.	
40	OEMs declaration certificate	Regarding their genuine, have their own manufacturing setups and Intellectual Property Rights IPR for the hardware(s)/software(s), and shall not have 3rd party manufacturing from any company blacklisted in India or abroad (due to proven backdoor access and data vulnerability) or any company sharing land border with India. The Proposed product should not be Third party manufacturing/contracting/ assembling / ODM .	
41	OEM Declaration	MANUFACTURER AUTHORISATION CERTIFICATE [MAF] from camera OEM should be produced in the name of OEM supplying the cameras. [MAF format Attached] All The cameras from same OEM. Proposed camera OEM must be full time member of ONVIF and	

		should not be blacklisted by ONVIF. [Reference Documents form ONVIF website]. OEM should not be blacklisted or barred by any Ministry of Government of India or globally or any of the Government / PSUs or any other government department at the time of bidding. The Camera OEM should have more than 10 years direct presence in India. The camera OEM should be in Surveillance business more than 15 Years from date of RFP.	
42	Intellectual Rights	The Intellectual Property Rights (IPR) of all manufactured final product and source code of all software including camera firmware should not reside in countries sharing land borders with India, until unless specifically allowed by the Government of India and is registered with the Competent Authority of Government of India.	
43	ISO Certificate	ISO 9001 ,ISO 14001, ISO 27001, 2011/65/EU ,IECQ QC 080000:2017	
44	OEM Declaration	OEM need to confirm that the Cameras etc., shall not be installed with standards like - GB28181, GB/T28181-2011, GB/T 28181-2011, GBT 28181-2011, GBT28181-2011, GB/T28181-2016, etc., protocols/standards and there shall be no option in the camera web page/settings to activate or deactivate such protocols/standards any of their version(s) or any such protocol which allow certain organizations to bypass all security parameters and look into the devices directly.	
45	OEM Declaration	OEM of Camera should be Fully Compliant to Section 889 of National Defence Authorization Act- NDAA . OEM undertaking is required stating that "NDAA Section 889 compliant products and does not have OEM, ODM and JDM relationships with the blacklisted vendors in the NDAA and do not use or deploy critical components including SoCs produced by NDAA banned component" vendors	

2) DOME CAMERA (FOR INDOOR USE)

Edge based AI Dome Camera- 5mp Camera			
Sl. No	**Parameter**	**Technical Specification**	**Compliance (Yes/No)**
1	**Make**		
2	**Model**		
3	Image Sensor	1/2.8" Progressive CMOS or better	
4	Resolution	2560x1920 (5MP) or better	

5	Lens	2.7 ~ 13.5 mm ,P- Iris ,Motorized, Vari-focal, Remote Focus,100.1° ~ 29.9° (Horizontal),71.8° ~ 22.4° (Vertical),135.2° ~ 37.4° (Diagonal),	
6	Shutter Time	1/30,000s s to 1/16 sec or better	
7	WDR	120dB or better	
8	Removable IR-cut Filter for Day/Night Settings	Yes	
9	S/N Ratio	68 db or better	
10	Minimum Illumination	0.04 lux @ F1.8 (Color) <0.005 lux @ F1.8 (B/W) 0 lux with IR illumination on	
11	Pan Range, Tilt Range, Rotation Range	±175°,80°,±175°	
12	Digital Zoom	16 X or better	
13	IR Illuminators	Built-in IR illuminators, effective up to 50 meters with Smart IR III, IR LED*4	
14	On-board Storage	Seamless Recording to MicroSD/SDHC/SDXC card slot, support upto 1TB. 256 GB SD Card class need to supplied at time of bidding	
15	Compression	H.265, H.264 & MJPEG	
16	Video Frame Rate	30 fps @ 2560x1920,60 fps @ 1920x1080 or better	
17	Video Streams	3 video streams (Up to 8 configurable profiles)	
18	Video Streaming	Adjustable resolution, quality and constant bit rate control, Smart Stream III	
19	Image Settings	video title and time stamp overlay, video orientation anti-overexposure, VCA-based Smart IR III, white balance, brightness, contrast, saturation, sharpness, gamma curve , defog, 3DNR, EIS (built-in gyro sensor), BLC, HLC, exposure level, iris adjustment, exposure time, gain control, iris mode, Privacy mask, pixel calculator, Scheduled profile settings, AI Power image enhancement(Smart IR-III)	
20	Audio Capability	Two-way Audio (full duplex)	
21	Audio Compression	G.711, G.726, MPEG-2 AAC-LC	
22	Audio Interface	External microphone input, Built-in microphone	
23		External line output	
24	Users	Live viewing for up to 10 clients or better	

25	Protocols	802.1X, ARP, Bonjour, CIFS/SMB, DDNS, DHCP, DNS, FTP/SFTP, HTTP/HTTPS, ICMP, IGMPv3, IPv4, IPv6, NTP, PPPoE, QoS (CoS/DSCP), RTSP/RTP/RTCP, SMTP, SNMP, SSL, TCP/IP, TLS 1.2, UDP, UPnP	
26	Security	Access list, Account block , Audit log, Configurable password strength protection, CSRF protection, Digest authentication, HTTPS , IEEE 802.1x, Secure boot, Session timeout, Signed firmware, Brute force attack event, Cyberattack event, Quarantine event , User access log, User account management, Built in Cybersecurity in camera	
27	Interface	10 Base-T/100 Base-TX Ethernet (RJ-45)	
28	ONVIF	Profiles G,S,T and Camera OEM should be full membership of ONVIF and it is available on onvif website	
29	Cybersecurity	Embedded in Camera	
30	Non -Hisilicon SOC	Yes	
31	Smart Motion Detection	video motion detection (Five -Window), People detection, Vehicle detection, Time filter	
32	Edge based Analytics	Intrusion detection, Loitering detection, Line crossing detection, Unattended object detection, Missing object detection, Face detection, Crowd detection	
33	Vision Object Analytics	Object Detection: People, Vehicle (4-wheeled, 2-wheeled); Attribute Extraction: People (gender, clothing color, bag, hat), Vehicle (bike, bus, car, motorcycle, truck, color); Re-Search Extraction; Path Extraction	
34	Compute Capability	SoC with built-in hardware deep learning accelerator	
35	Alarm Triggers	Audio detection, camera tampering detection, brute force attack event, cyberattack event, quarantine event , digital input, manual trigger, motion detection, periodical trigger, recording notification, SD card life expectancy, shock detection, system boot	
36	Alarm Events	Event notification via audio clip, camera link, digital output, email, HTTP, FTP/SFTP, NAS server, SD card	
37		File upload via email, HTTP, FTP/SFTP, NAS server, SD card	
38	IP Connectors	RJ-45 cable connector for 10/100 Mbps PoE network connection	
39		Audio line input	

40		Audio line output	
41		DC 12V power input	
42		Digital input *2	
43		Digital output *2,Micro USB	
44	Power Input	AC 24V DC 12V, IEEE 802.3af PoE Class 0 (Power Redundancy)	
45	Power Consumption	12.95 W or better	
46	Operating Temperature & Humidity	Starting Temperature: -30°C ~ 60°C (-22°F ~ 140°F) Working Temperature: -40°C ~ 60°C (-40°F ~ 140°F) (IR off) -40°C ~ 50°C (-40°F ~ 122°F) (IR on) ,98% RH (non-condensing)	
47	Safety Certifications for Camera	EMC: CE (EN 55032/EN 55035 Class B, EN 50121-4), FCC (FCC Part 15 Subpart B Class B), IC (ICES-003 Issue 7); Safety: UL (UL 62368-1), CB (IEC/EN 62368-1, IEC/EN 60950-22, IEC/EN 62471), LVD, (EN 62368-1) Environment: IK10+ (IEC 62262), IP66/67 (IEC 60529), NEMA (NEMA 250 Type 4X), IEC 60068-2-11, IP6K9K (ISO 20653); IA: BIS (IS 13252)	
48	Flash/RAM	8GB/2GB	
49	NDAA & TAA Compliant	Yes	
50	Cybersecurity	Built in Camera	
51	MTBF	More than 300,000 hrs	
52	Detect (25PPM/ 8PPF)	Wide: 64.4 m (211.2 ft) Tele: 196.6 m (645.2 ft)	
53	Observe (63PPM/ 19PPF)	Wide: 25.7 m (84.4 ft) Tele: 78.7 m (258.1 ft)	
54	Recognize (125PPM/ 38PPF)	Wide: 12.8 m (42.1 ft) Tele: 39.3 m (129.0 ft)	
55	Identify (250PPM/ 76PPF)	Wide: 6.4 m (20.9 ft) Tele: 19.6 m (64.5 ft)	

3) IP PTZ CAMERA

SPECIFICATION OF 4MP IP PTZ CAMERA			
Sl. No	**Parameter**	**Technical Specification**	**Compliance (Yes/No)**
1	Make		
2	Model		
3	Image Sensor	1/2.8" Progressive CMOS or better	
4	Resolution	2560x1920 (5MP) or better	

5	Lens Type	30x Optical Zoom, Auto Focus or better	
6	Focal Length	f = 4.94 ~ 148.24 mm [/- 1mm] or better,54.1° ~ 1.9° (Horizontal),41.2° ~ 1.4° (Vertical) 65.7° ~2.4° (Diagonal),F1.3 ~ F4.6,DC-iris	
7	Auto-iris	DC-iris	
8	Shutter Time	1/1 sec. to 1/100,000 sec	
9	Removable IR-cut Filter for Day /Night Settings	Yes	
10	IR Illuminators	Built-in IR Illuminators up to 200 meters with Smart IR, IR LED*8 or better	
11	Minimum Illumination	0.03 lux @ F1.3 (Color)	
12		0.005 lux @ F1.3 (B/W)	
13		0 lux with IR illumination on	
14	Pan Speed	0~ 450°/s	
15	Pan Range	360° endless	
16	Tilt Range	-20° to 90° (auto flip)	
17	Tilt Speed	0~ 450°/s	
18	Preset Locations	256 Preset locations,128 presets per tour	
19	Pan/Tilt/Zoom Functionalites/e-PTZ	25x digital zoom or more	
20		Auto Pan mode	
21		Auto Patrol mode	
22		Mechanical Auto flip	
23	Storage	Seamless Recording to MicroSD/SDHC/SDXC card slot. The Camera should be support upto 1 TB SD Card class 10 and recording to network-attached storage (NAS). 256 GB SD Card class need to supplied at time of bidding	
24	Video Compression	H.265, H.264, MJPEG	
25	Video Frame Rate	30 fps @ 2560x1920 60 fps @ 1920x1080	
26	Video Streams	Min3 video streams and configurable more than 8 Profiles or better	
27	S/N Ratio	Minimum 70 dB or better	
28	WDR	120 dB or better	
29	Video Streaming	Adjustable resolution, quality and constant bit rate control, Smart Stream III/Zip Stream	
30	Image Settings	Video title and time stamp overlay, video orientation , anti-overexposure, white balance, brightness, contrast, saturation, sharpness, gamma curve, defog, 3DNR, HLM, EIS, scene mode , BLC, HLC, gain control, 3DPrivacy mask (24) ; Scheduled profile settings, Pixel Calculator	
31	Audio Capability	Two-way audio	
32	Audio Compression	G.711, G.726	
33	Audio Interface	External microphone input	
34		External line output	
35	Unicast User	Live viewing for more than 7 clients or better	
36	Security	Access list, digest authentication, HTTPS, IEEE 802.1x, password protection, signed firmware,	

		brute force attack event, cyberattack event, quarantine event, user access log, user account management, embedded cybersecurity	
37	Protocols	802.1X, ARP, Bonjour, CIFS/SMB, DDNS, DHCP, DNS, FTP, HTTP, HTTPS, ICMP, IGMPv 3, IPv 4,IPv 6, NTCIP, NTP, PPPoE, QoS , RTSP/RTP/RTCP,SMTP, SNMP, SSL, TCP/IP, TLS 1.2, UDP, UPnP	
38	Interface	10 Base-T/100 Base TX/1000 Base TX Ethernet (RJ45)	
39	ONVIF	Profiles G,S,T and Camera OEM should be full membership of ONVIF and it is available on onvif website	
40	Video Motion Detection	Yes	
41	Analytics	Edge base Analytics-Intrusion detection, loitering detection, line crossing detection, face detection	
42		Vision Object Analytics-Object Detection: people, vehicle 4 wheeler & 2-wheeler, Attribute Extraction- people (gender, color, bag, hat), vehicle (bike, bus, car, motorcycle, truck, color); Re-Search Extraction; Path Extraction	
43	Compute Capability	SoC with built-in hardware deep learning accelerator	
44	Event Trigger	Audio detection, camera tampering detection, brute force attack event, cyberattack event, quarantine event , digital input, manual trigger, motion detection, periodical trigger, recording notification, SD card life expectancy, smart tracking trigger	
45	Event Action	Event notification via audio clip, digital output, email, HTTP, FTP, NAS server, SD card ,File upload via email, HTTP, FTP, NAS server, SD card, trigger track, trigger patrol,	
46	IP Connectors	RJ-45 cable connector f or 10/100 Mbps PoE network connection	
47		Audio line input	
48		Audio line output	
49		DC 48V power input	
50		AC 24V power input	
51		Digital input*2	
52		Digital output*1	
53	Power Input	IEEE 802.3bt Class 6 PoE, DC 48V, AC 24V (Dual Power supply)	
54	Power Consumption	PoE: Max. 51W/26W (IR on/off) DC 48V: Max. 51W/26W (IR on/off) AC 24V: Max. 51W/26W (IR on/off)	
55	Certifications	CE (EN 55032 Class A, EN55035, EN50121-4), FCC (FCC Part 15 Subpart B Class A) ICES-003:2020 Issue7, Class A, UL (UL 62368-1), IEC/EN 62368-1, IEC/EN 60950-22, IEC/EN 62471 ,IK10 (IEC 62262), IP66 (IEC 60529), NEMA (NEMA 250 Type 4X, BIS (IS 13252)	
56	Operating	-40°C ~ 55°C	

	Temperature		
57	Humidity	98% or better	
58	Flash/RAM	8GB/2GB	
59	NDAA /Non Hisilicon SOC	Compliant	
60	Cybersecurity	Embedded in Camera	
61	MTBF	More than 300,000 hrs	
62	Detect (25PPM/ 8PPF)	Wide: 104.1 m (341.5 ft) Tele: 2969.8 m (9743.4 ft)	
63	Observe (63PPM/ 19PPF)	Wide: 41.3 m (135.5 ft) Tele: 1178.5 m (3866.4 ft)	
64	Recognize (125PPM/ 38PPF)	Wide: 20.8 m (68.2 ft) Tele: 594 m (1948.6 ft)	
65	Identify (250PPM/ 76PPF)	Wide: 10.4 m (34.1 ft) Tele: 297 m (974.3 ft)	

4) **VEHICLE NUMBER PLATE READER SENSOR**

Sl. No	Parameter	Technical Specification	Compliance (Yes/No)
1	sensor	1920 x 1200 @ 30 fps; progressive scan Monochrome CCD LPR camera; global shutter speed	
2	Capture range	3 - 45 m	
3	LPU Processor	Processor – min.1.6 GHz Intel Atom E3950 Quad core (2MB L2 cache), 4GB RAM. Or higher	
4	OS	Linux / windows.	
5	Illuminator	Pulsed LED illuminator for effective use in 0 lux (total darkness) Environments	
6	Context camera sensor	1920 x 1200 @ 30 fps; color; global shutter	
7	Operating temperature	(-40°C to 65°C) ambient	
8	On-board analytics	Vehicle type, vehicle color, speed estimation, direction of travel, virtual loop, etc.	
9	Power supply	Should support both • POE +/ PoE++ (802.3bt) • 24V DC input	
10	Sealing (water/dust protection)	IEC 60529: IP66/IP67/IP 68	
11	Still image compression	JPEG compression for VRNR and Context still images	
12	Data interface	LAN: 1 x 10/100/1000 Base-T Ethernet port	
13	Video streaming	H.264 @ up to 30 fps	
14	Vibration & shock	IEC 60068-2-64: 5~100Hz | 0.5 g rms IEC 60068-2-27: 10g | 16ms half-sine MIL-STD-810H §514.8	

15	Impact	IEC 62262: IK09	
16	Electromagnetic immunity & emissions	FCC | ICES-003 Issue 4 | CISPR32 / EN55032 | CISPR35 / EN55035	
17	EMC directive (CE marking)	2014/30/EU	
18	Safety	IEC/EN 62471.	
19	External I/Os	2 inputs / 2 outputs	
20	TCP/IP Communication	Support both IPV4 & IPV6	
21	Performance	Cameras must feature edge-based machine learning capabilities and achieve a high accuracy rate (Out of 100nos of reads 95 nos of read must be corrects) in vehicle number plate reading, during both day and night conditions.	

5) SPECIFICATIONS OF UNIFIED COMMAND & CONTROL AND VMS SOFTWARE

Sl. No.	Technical Specifications	Compliance (Yes / No)
	General	
1	The Unified Command and Control Platform (UCC) should be an enterprise class IP-enabled Cloud ready application. The UCC should support the seamless unification of various Public Safety elements like IP video management system (VMS), Automatic number/licence plate reader system (ANPR/ALPR), Incident management, Emergency response system. Criminal tracking, record management, Traffic management solutions under a single platform with scope for future scalability. The UCC user interface (UI) applications should present a unified user interface for the management, configuration, monitoring, co - relation, intelligence and reporting of various embedded systems and associated edge devices.	
2	The platform must be Cloud ready from day 1 and must have the ability to host either in total or some of the modules in a private cloud environment approved by “MEITY”.	
3	The platform must have native failover. The failover must support both local & over geographical redundancy for all the modules outlined under the UCC platform. The OEM must ensure scalability and high availability.	
4	The UCC platform must be a true unified management experience for critical infrastructure, simplifying control room operation and system integration, minimizing total cost of ownership, and increasing operational efficiency critical to rapid decision-making.	
5	The UCC Platform should maximize real-time monitoring and control efficiency from one workstation through the synchronized control of high-resolution blueprints, images, streaming camera	

	data, and system alerts which allows for interaction between all relevant data	
6	It should allow simple and accessible Integration with other independent control systems through a single Unification point with consistent user interface and better operational efficiency.	
7	UCC should be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform	
8	UCC system should provide a real time Common Operating Picture (UCC) of the area involving all agencies using a simple Operator / User friendly interface	
9	The system should support various sensors like Cameras, GPS, Voice devices, Storage devices, Sensor inputs from other Utility applications/ systems	
10	The UCC platform should provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making.	
11	The UCC platform should provide a cross-agency collaboration tool to support instant communication between various user groups and authorities.	
UCC Architecture:		
1	The Application should be an IP enabled solution. All communication between the servers and other clients should be based on standard TCP/IP protocol and should use TLS encryption with digital certificates to secure the communication channel.	
2	The Application should protect against potential database server failure and continue to run through standard off-the-shelf solutions.	
3	The Application should support up to one thousand instances of Clients connected at the same time. However, an unrestricted number of Clients can be installed at any time	
4	The Application should support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.	
5	The UCC Application should support native and off-the-shelf failover options without any dependency on external application for both Hardware and Application.	
Native Map module (Both GIS and Offline Maps):		
1	The GIS MAP should support the standard file formats defined by the Open Geospatial Consortium (OGC) and feature to export these maps in PDF, JPG and PNG should be available	
2	It should be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.	
3	The UCC should provide a map centric interface with the ability to Command & Control all the system capabilities from a full screen map interface.	
4	It should be possible to span the map over all screens of the UCC client station. In the scenario where the map is spanned over all the screens of the UCC client station it should be possible to navigate	

	the map including pan and zoom, and the map's moves should be synchronized between all screens. Spanning the map over multiple screens must provide the same Command & Control capabilities than in a single screen display.	
5	The GIS MAP should provide the ability to display layer of information in Keyhole Mark-up Language (KML) format.	
6	It should be possible to monitor the state of entities on the map. It should be possible to customize the icons of any entities represented on the map.	
7	It should be possible to select a location by drawing a zone of interest on the GIS MAP, and to display all the entities that are part of that zone of interest at once.	
8	The user should be able to select and display the content of multiple UCC entities on the map in popup windows	
9	The GIS MAP should provide the following search capabilities but not limited to these only:	
10	Search within the map by entity name, street name, or point of interest.	
	Drag and drop entities from the UCC to the map to centre their location.	
	Map to support event-based response actions for decision making in case of any emergency / critical situation	
	CCTV feeds to be viewed on the Map in case of any event triggers	
Alarm Management		
1	The UCC should support the following Alarm Management functionality	
2	Create and modify user-defined alarms. An unrestricted number of user-defined alarms should be supported	
3	Assign a time schedule or a coverage period to an alarm. An alarm should be triggered only if it is a valid alarm for the current period	
4	Set the priority level of an alarm and its reactivation threshold.	
5	User should have capability to define whether to display live or recorded video, still frames / create snapshot or a mix once the alarm is triggered.	
6	Provide the ability to group alarms by source and by type.	
7	Define the recipients of an alarm. Alarm notifications should be routed to one or more recipients. Recipients should be assigned a priority level that prioritizes the order of reception of an alarm.	
8	The workflows to create, modify, add instructions and procedures, and acknowledge an alarm should be consistent for various systems.	
9	The UCC should also support alarm notification to an email address or any device using the SMTP protocol.	
10	The ability to create alarm-related instructions should be supported through the display of an alarm event.	
11	The user can acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.	
12	The user should able to spontaneously trigger alarms based on	

	something he or she sees in the UCC system Dashboard.	
13	UCC platform should generate Notification, Alert and Alarm messages as per the incidences / events that are received, that should be visible within the Dashboard and the Field Responder Mobile App or web services/portal if required.	
14	All system messages (notifications, alerts and alarms) should always be available from the Notifications View, which provides controls that operator can use to sort and filter the messages that it displays	
Reporting:		
46	The UCC should support report generation (database reporting) for various systems Unified into the platform	
47	The workflows to create, modify, and run a report should be consistent for all systems	
48	The UCC should support the following types of reports	
49	Alarm reports.	
50	Video-specific reports (archive, bookmark, motion etc.)	
51	Configuration reports	
52	/VRNR-specific reports (mobile / VRNR playback, hits, plate reads, reads/hits per day, reads/hits per /VRNR zone, and more).	
53	Generic Reports, Custom Reports and Report Templates	
54	The user should be able to customize the predefined reports and save them as new report templates. There should be no need for an external reporting tool to create custom reports and report templates. Customization options should include setting filters, report lengths, and timeout period. The user should also be able to set which columns should be visible in a report. The sorting of reported data should be available by clicking on the appropriate column and selecting a sort order (ascending or descending).	
55	The UCC should support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.	
56	The user should be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.	
57	The UCC should support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients	
Real Time Dashboard:		
1	Real time dashboard should provide the real-time information about the security situation so called Situational Awareness for the Authorities and senior officials in a single go	
2	The Monitoring UI should dynamically adapt to what the operator is doing. This should be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.	
3	Widgets should be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions. UCC software should have drag and drop facility for all widgets for	

	user to move the required alerts and other windows on priority basis.	
4	Analysts / Operators should be allowed to view dashboards if they are granted the appropriate privilege. Modification to the dashboards should also be allowed to users granted the appropriate privilege.	
5	Dashboard widget types should be: Image: provides the ability to display an image (JPG, PNG, GIF, and BMP) on a dashboard. Text: provides the ability to display a text on a dashboard. The text style should be configurable, so font, size, colour, and alignment can be specified by the user. Tile: provides the ability to display any entity of the USP inside of a tile. Web page: provides the ability to display a URL on a dashboard. Entity Count: provides the ability to display the total number of a specific entity type in the UCC	
6	Reports: provides the ability to display the results of any saved reports in the system. The results should be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.	
Threat Level Indication:		
1	UCC should display the threat level based on the number of alerts and criticality of the alerts using color coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts. It should be possible to activate various threat situations from Web / Mobile client application for those users with appropriate privileges	
Incident Management & Reporting:		
1	The UCC should support the configuration and management of events. A user should be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.	
2	The UCC should receive all incoming events from one or more Unified Systems. The UCC should take the appropriate actions based on user- define event/action relationships.	
3	Incident reports should allow the security operator to create reports on incidents that occurred during a shift. Both video-related and other Unified Systems related incident reports should be supported.	
4	The operator should be able to create standalone incident reports or incident reports tied to alarms.	
5	The operator should be able to link multiple video sequences to an incident, access them in an incident report.	
6	It should be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.	
7	Incident reports should allow the creation of a custom form on which to input information on an incident.	
8	Incident reports should allow entities, events, and alarms to be added to support at the report's conclusions	

9	Reporting function is part of Command & Control dashboard visualization tool. It should provide information about status of the Command & Control on managing the security incidents across the locations. Reporting function should enable operator to create reports in either graphical format or flat tabular format. Reports should be created automatically or manually by operator whenever required. The reports should be generated and exported as a Microsoft word excel format or an acrobat format by operator	
10	It should be possible to generate a report from UCC interface based on the profiles defined for the Incident management and associated tools defined with in IM Module. a. The profile report should be exportable and printable. b. Profile reports should allow filtering on profile identifier, initiators, recipient, and modification time. c. Columns for the profile reports should be configurable	
Configuration User Interface:		
1	The Configuration UI application should allow the administrator or users with appropriate privileges to change the system configuration	
2	The configuration of all embedded systems should be integrated and accessible via the Configuration UI as per the authorizations of the user	
3	The Configuration UI should have a home page with single-click access to various tasks.	
4	The Configuration UI should include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.	
The Configuration UI should include a static reporting interface to:		
1	View historical events based on entity activity. The user should be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view.	
2	View audit trails that show a history of user/administrator changes to an entity.	
3	Common entities such as users, schedules, alarms and many more, can be reused by all embedded systems in platform	
4	The application must have single user unified interface for configurations of all the systems of Video, /VRNR and Emergency response.	
Smartphone and Tablet App General Requirements:		
1	The UCC should support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps should communicate with UCC over any WIFI or mobile network connection.	
2	All the communication between the mobile apps and UCC platform will be on HTTP and by adding TLS encryption.	

Mobile app Functionalities:		
1	(a). Ability to change the password of the user of the mobile app. (b). Ability to execute assigned tasks/ actions configured in the user profile. (c). Ability to view below minimum edge devices Unified with the UCC platform: i. Cameras ii. Cameras Alerts iii. GIS and Offline Maps iv. Ability to navigate the system hierarchical view of the edge devices & entities with ability to search entities in the system. (d). Ability to have GIS maps on the app and access the live, recorded video feeds and alarms directly on mobile app. (e). Ability to view live and recorded video from the cameras. (f). Ability to use the camera of the smartphone and stream a live video feed to Command centre from field operators. (g). Ability to receive push notifications to notify mobile operators that an alarm was received. (h). Ability to view all active alarms assigned to the mobile operator (I). Ability to perform action on an alarm such as acknowledge, forward, or alternate-acknowledge an active alarm. (j). Ability to search for devices like cameras or locations on the integrated GIS map. (k). Any other features required / customization in existing facility should be made available.	
System Health Monitor:		
1	The UCC should monitor the health of the system, log health-related events, and calculate statistics.	
UCC Audit and User Activity Trails		
1	The UCC should support the generation of audit trails. Audit trails should consist of logs of operator/administrator additions, deletions, and modifications	
2	Audit trails should be generated as reports. They should be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods should also be possible.	
3	For entity configuration changes, the audit trail report should include detailed information of the value before and after the changes	
4	The UCC should support the generation of user activity trails. User activity trails should consist of logs of operator activity on the UCC such as login, camera viewed, badge printing, video export, and more.	
5	The UCC should support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.	
Third Party System Unification:		
1	Directory service like MS – AD or Similar integration should permit	

	the central user management of the UCC users, user groups and other Access control groups.	
2	The UCC should support multiple approaches to integrating third party systems and other software application. These should include: Software Development Kits (SDKs), Driver Development Kits (DDKs), REST-based Web Service SDK and RTSP Service SDKs, Application Programming Interface (API)	
3	There should be provision in UCC to support custom development for the platform	
4	The SDK/APIs should provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.	
Cyber Security Requirements:		
1	The UCC Application should be an IP enabled solution. All communication between the Servers, Clients and external systems should be based on standard TCP/IP protocol and should use TLS encryption with digital certificates to secure the communication channel.	
2	The Application should limit the IP ports in use and should provide the Administrator with the ability to configure these ports.	
3	The VMS system Unified with the UCC application should support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests should be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.	
4	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.	
Video Management System (VMS)		
1.	The Video Management System (VMS) should be an enterprise class IP-enabled application. The VMS should support the seamless unification of various Public Safety elements including Access Control, Communication Management and Alarm Management. The VMS user interface (UI) applications should present a unified security interface for the management, configuration, monitoring, intelligence and reporting of various embedded systems and associated edge devices.	
2.	All communication between the servers and other clients should be based on standard TCP/IP protocol and should use TLS encryption with digital certificates to secure the communication channel.	
3.	The proposed Video Management System (VMS) should provide a complete end-to-end solution for security & surveillance application. The VMS should be an enterprise class IP based application with Server-client architecture. The VMS should support cameras using the industry standards ONVIF Profile S, G, T	

	and M. The VMS should have Management Servers, Recording Servers and Client Interface as integral part of the solution.	
4.	The Video Management Server should provide centralized management of all IP cameras. The database should support more than 50000 cameras / IP end points and scalable to 20000.	
5.	The VMS platform should provide a dashboard functionality.	
6.	The Proposed VMS solution should support native failover within application with no dependency on any external application for both hardware and application redundancy. The native failover architecture must be for both management and recording servers.	
7.	The Failover and Fallback Management Server will be on hot standby, ready to take over during the primary Management Server fails. No manual action from the user will be required. The failover time will not be beyond 1 Min and there should not be any loss in the Live and Recorded Videos of the connected cameras.	
8.	The VMS server should support disaster recovery scenarios where a server can be in another geographic area (or building) and only take over if Primary server becomes offline.	
9.	The VMS and its associated clients should support Direct Multicast of video streams from the Cameras. The application should redirect video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture should not use multicast streaming via recording servers or any other servers. This will achieve bandwidth usage optimization in the network usage and increase the overall compute capacity of recording servers.	
10.	The Application should be capable to handle both IP v4 and IP v6 Unicast and Multicast traffic with both PIM - SM and PIM - DM support.	
11.	The application management server should not have any limitation on the no of recording servers added on one single management / failover server. Any limitations must be clearly specified by the bidder.	
12.	There should not be any dependency on the end point MAC address for licensing for ease of operations.	
13.	The VMS should have the ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system.	
14.	Ability to locate the mobile app user on map and provisioning to message and collaborate in real time with the central command center or field staff.	
Alarm Management:		
15.	I. Set the priority level of an alarm and its reactivation threshold. II. User should have capability to define whether to display live or recorded video, still frames / create snapshot or a mix once the alarm is triggered.	

	III. Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode or display live and recorded video in different video tile side by. IV. Provide the ability to group alarms by source and by type. V. Define the recipients of an alarm. Alarm notifications should be routed to one or more recipients. Recipients should be assigned a priority level that prioritizes the order of reception of an alarm. VI. The VMS should also support alarm notification to an email address. VII. The ability to create alarm-related instructions should be supported through the display of an alarm event. VIII. The user can acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze. IX. The user should be able to spontaneously trigger alarms manually based on something he or she sees in the VMS Dashboard.	
16.	Real time dashboard should provide the real-time information about the security situation so called Situational Awareness for the responders in a single go.	
17.	The VMS Monitoring UI should dynamically adapt to what the operator is doing. This should be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.	
18.	Reports: provides the ability to display the results of any saved reports in the system. The results should be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.	
19.	The user should be able to customize the predefined reports and save them as new report templates. Customization options should include setting filters and report lengths. The user should also be able to set which columns should be visible in a report. The sorting of reported data should be available by clicking on the appropriate column and selecting a sort order (ascending or descending).	
20.	The VMS platform should have native extensive dashboard functionality with high flexibility to modify the dashboards based on various parameters including creating alarms and incidents streamed through the edge analytics of the cameras.	
21.	The platform should support report generation (database reporting) for various systems unified into the platform from single interface.	
22.	The platform should support comprehensive data filtering for most reports based on entity type, event type, event timestamp, and more.	
	System Health Monitor	
23.	The VMS should monitor the health of the system, log health-related events, and calculate statistics.	
24.	Detailed system care statistics should be available through a	

	dashboard providing health metrics of the entities and roles, including Uptime and mean-time-between- failures	
	Cyber Security Requirements:	
27.	The VMS Application should be an IP enabled solution. All communication between the Servers, Clients and external systems should be based on standard TCP/IP protocol and should use TLS encryption with digital certificates to secure the communication channel.	
28.	The Application should limit the IP ports in use and should provide the Administrator with the ability to configure these ports.	
29.	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.	
30.	The OEM of VMS application should have an online or offline Cyber Security emergency response center to update on latest vulnerabilities and provide needed assistance during any cyber-attacks on the system. Details of response center must be available on the OEM global website.	
31.	The OEM of VMS must be ISO 27001 certified. Copy of the Certificate must be submitted along with the technical bid document	
32.	The VMS platform must have UL 2900-2-3 Level 3 Cyber Security certification and bidders must provide the same along with technical bid	
33.	The VMS platform should have Cyber Security SOC Type 2 report and bidders must provide the same along with technical bid	
34.	The proposed platform must be GDPR compliant for data privacy	

6) SPECIFICATIONS OF INCIDENT MANAGEMENT (IM) SOFTWARE

Sl. No.	Specification	Compliance (Yes/No)
1.	The IM MODULE shall be seamlessly embedded and must be a native module in the UCC PLATFORM	
2.	The UCC PLATFORM and IM MODULE shall be forward compatible so upgrade of one does not prevent from using the other.	
3.	The IM MODULE shall be seamlessly compatible with the UCC PLATFORM and any of its sub-components including VMS, /VRNR, FRS, Video Analytics, Big Data Co relation tool and external SDK / API integrations with 3rd party systems	
4.	The IM MODULE shall offer the following operational tools: Incident management. Document management Rules Engine Workflow Automation Standard Operating Procedures Incident monitoring operator interface	

	Incident reports	
5.	The IM MODULE shall provide situational intelligence to the operator with a map-centric approach and detailed overview of incident data, combining incident history, operator comments, workflow and operator action logs, standard operating procedures, relevant live and playback video, and an aggregated events sequence of the incident	
6.	The IM MODULE shall log all configuration changes in an audit trail with before and after configurations.	
7.	The IM MODULE shall log all the user activities that are executed during the time that an incident is active.	
8.	The IM MODULE shall provide the ability to configure incidents in a test mode that would allow user with the appropriate privilege to validate different parameters before activating the incident configuration	
9.	The IM MODULE shall be the interface that displays all situations as incidents.	
10.	The IM MODULE shall provide the ability to trigger incidents manually or automatically, based on a correlation of events such as	
11.	a. An incident shall be the holistic description of the situation and support the following attributes: Visual: · Colour · Icon. b. Incident management shall provide the ability to customize incident types using a set of imported icons. c. Incident category shall allow an operator to organize incident types in a logical tree d. The location can be an entity (camera, door, zone, area) or a geographical coordinate. e. A priority level f. A description g. States h. Standard operating procedures. i. History of activities. j. Attached Entities, entities related to the source of events triggering the incident shall be automatically associated to the incident. k. Attached documents. Documents and URLs providing more information or guidance on the incident and its management	
12.	The Incident management shall provide management of incident ownership. It shall be possible to explicitly request or release the ownership of an incident. Ownership of an incident shall be provided immediately to an operator who starts working on an incident.	
13.	A supervisor shall be able to view all incidents that are under his supervision and see the ownership of each incident. In the same view, the supervisor shall also be provided with real-time information about who is currently monitoring an incident	

14.	The IM MODULE shall notify the supervisor when an operator skips a step in the standard operating procedure (SOP).	
15.	For each incident, it shall be possible to open the incident details. The incident details will open on a configurable screen and provide, based on the incident type configuration, the following information: 1. A layout of all live and playback video related to the incident, including the camera associated to the source and location of the incident, as well as the local map centered on the incident location. 2. History of the incident including: a. All events related to the incident b. System workflow activities c. Operator actions for the incident d. Comments about the incident	
16.	Operators shall be able to perform the following actions: 1. Change the incident state. 2. Forward the incident. 3. Transfer the incident. 4. Edit the incident: a. Change the description b. Change the priority level c. Release the ownership 5. Attach additional entities to the incident. 6. Link related incidents. 7. Attach a document as a URL link to the incident	
17.	The IM MODULE shall provide the ability to dispatch an incident to a user or group of users. Dispatching an incident to a restricted number of users will secure the access to information.	
18.	Incident supervisors shall be able to see all sub-incidents associated with a main incident.	
19.	The IM MODULE shall offer a task to manage and generate reports. The ability to run a report is a user privilege.	
20.	It shall be possible to query the incident history filtering by: a. Incident type b. Incident state c. Location d. Priority e. Trigger time range f. Incident owner g. Description h. Combination of any of the above mentioned filters. Over and above if more parameters are captured the facility to search on those parameters should be provided.	
21.	The result of a report query shall provide a list of incidents as well as a visual of these incident locations on the map. When more than one incident is reported at the location, the GUI will cluster these incidents on the map.	

22.	For closed incidents, the incident shall be in read-only mode with the exception of adding links to related incidents.	
23.	The Report task shall also report the user activity log of the UCC PLATFORM for the time in which the operator was owner of the incident and was monitoring it, in order to provide a view of all actions taken towards the resolution of this incident.	
24.	The IM MODULE shall offer all reports in a visual presentation format (such as pie charts, lines, columns, and rows) native within the platform with no necessary for additional external tools or software modules.	
25.	The IM MODULE shall support the following report formats: a.HTML b.PDF c.XML d. XLS/CSV	
26.	A document shall be automatically attached to an incident if the document properties match the incident properties. The following properties shall be available: a. Incident type b. Schedule c. Location. Location can be an entity or an area. d. User or user group of the operator monitoring the incident	
27.	The IM MODULE shall offer the ability to automatically link a document to a step in a standard operating procedure	
28.	Document Management shall provide a file system to store all documents as well as the document URLs for the use of third-party file systems.	
29.	The Incident Management module should have facility to configure a sequence of events using logical AND /OR /NOT operators to trigger and incident	
30.	Configuring the Rules Engine shall be graphical /the rules could be imported.	
31.	It shall be possible to configure a complex sequence of rules by applying the occurrence, the interval, and event filtering.	
32.	It shall also be possible to script the rules in advance and import them into the system later.	
33.	The IM Module shall provide a native Workflow Engine to automate the response to an incident type.	
34.	The IM Module shall provide a graphical workflow designer. No scripting competence shall be required to implement a workflow.	
35.	It shall be possible to define a workflow for each incident type. The workflow shall be a series of activities that are sequentially executed.	
36.	The IM Module shall provide guidance for operators in the form of a standard operating procedure (SOP) for the response to an incident type	
37.	The SOP shall be interactive and offer an operator-acknowledgement- audit for each SOP step.	

38.	The SOP shall be dynamic and provide the ability to adapt the next steps in a procedure based on the responses to previous steps in the procedure.	
39.	The IM Module shall provide the ability to skip a step of the SOP and request a justification for skipping the step.	
40.	Each step shall be optionally associated to a document in the form of a URL, or a document in a supported format (such as Word, PDF, or HTML).	
41.	The tool shall track the elapsed time for each step of the SOP, as well as the total elapsed time from the initial response to resolution and enable the authorities to determine the steps which are getting delayed and plan the training needs for the crime analysts and UCC PLATFORM operators.	
42.	The IM MODULE shall provide the ability to configure standard options when defining dynamic steps of the SOP.	
43.	A maximum delay shall be allowed for a user to initiate the procedure. Automated actions associated with this time to response threshold shall be configurable.	
44.	A minimum configurable time as per SOPs shall be allocated for a user to complete the procedure. Closing the incident before passing this time to resolution threshold shall trigger actions as per defined SOPs.	
45.	A visual indicator shall be displayed when maximum time to response or the maximum time to resolution for the incident is exceeded.	
46.	The UCC PLATFORM shall support report generation (database reporting) for various systems Unified into the platform	
47.	The workflows to create, modify, and run a report shall be consistent for all systems	
48.	The UCC PLATFORM shall support the following types of reports	
49.	Alarm reports.	
50.	Video-specific reports (archive, bookmark, motion etc.)	
51.	Configuration reports	
52.	NPR-specific reports (mobile NPR playback, hits, plate reads, reads/hits per day, reads/hits per NPR zone, and more).	
53.	Generic Reports, Custom Reports and Report Templates	
54.	The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).	
55.	The UCC PLATFORM shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.	

56.	The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.	
57.	The UCC PLATFORM shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients	
58.	Real time dashboard should provide the real-time information about the security situation so called Situational Awareness for the Authorities and senior officials in a single go	
59.	The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.	
60.	Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions. UCC PLATFORM software should have drag and drop facility for all widgets for user to move the required alerts and other windows on priority basis.	
61.	Analysts / Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to the dashboards should also be allowed to users granted the appropriate privilege.	
62.	Dashboard widget types shall be: Image: provides the ability to display an image (JPG, PNG, GIF, and BMP) on a dashboard. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, colour, and alignment can be specified by the user. Tile: provides the ability to display any entity of the USP inside of a tile. Web page: provides the ability to display a URL on a dashboard. Entity Count: provides the ability to display the total number of a specific entity type in the UCC PLATFORM	
63.	Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.	
64.	UCC PLATFORM should display the threat level based on the number of alerts and criticality of the alerts using color coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts. It should be possible to activate various threat situations from Web / Mobile client application for those users with appropriate privileges	
65.	The UCC PLATFORM shall support the configuration and management of events. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.	
66.	The UCC PLATFORM shall receive all incoming events from one or more Unified Systems. The UCC PLATFORM shall take the appropriate actions based on user- define event/action relationships.	

67.	Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and other Unified Systems related incident reports shall be supported.	
68.	The operator shall be able to create standalone incident reports or incident reports tied to alarms.	
69.	The operator shall be able to link multiple video sequences to an incident, access them in an incident report.	
70.	It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.	
71.	Incident reports shall allow the creation of a custom form on which to input information on an incident.	
72.	Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions	
73.	Reporting function is part of Command & Control dashboard visualization tool. It shall provide information about status of the Command & Control on managing the security incidents across the locations. Reporting function should enable operator to create reports in either graphical format or flat tabular format. Reports shall be created automatically or manually by operator whenever required. The reports should be generated and exported as a Microsoft word excel format or an acrobat format by operator	
74.	It shall be possible to generate a report from UCC PLATFORM interface based on the profiles defined for the Incident management and associated tools defined with in IM Module. a. The profile report shall be exportable and printable. b. Profile reports shall allow filtering on profile identifier, initiators, recipient, and modification time. c. Columns for the profile reports shall be configurable	

7) SPECIFICATION OF MANAGEMENT & RECORDING SERVERS

Recording & Failover Server Systems: with suitable capacity for management and recording video feeds for the CCTV camera as per the recording parameters decided by the end user. Vendor may note that storage calculation has to be taken & verified from Camera OEM. VMS OEM shall provide certification regarding offered Storage Server Solution meeting the requirement. Following is the indicative specification per storage server:

SL. No.	Parameter	Minimum Technical Specifications	Complied Yes/No
1	Application	Server compute for hosting application (VMS Recording Server appliance)	
2	CPU	1x Intel® Xeon® Silver 4410Y or better	
3	Mounting	2U rack mounted with sliding rails	
4	Memory	Min 32GB RAM	
5	Storage/ Hard Disk	Shall be RAID 5 Min as per the bandwidth storage calculation of the camera OEM.	
6		Keep Your Hard Drive Support to be provided	

7	OS Hard Disk	2x 480GB M.2 NVMe For OS & Application	.
8	PCI Slots	Up to 2x PCIe LP slots	
9	NICs	2x 1GbE RJ45 or better	
10	Power Supply	Platinum rated Dual, Hot-plug, Redundant Power Supply	
11	OS	Windows Server 2022	
12	Others	The appliance must be a turnkey solution with Video Management Software pre- installed and only camera and other licenses to be activated at site.	
13		The appliance should be extensively tested and hardened for security to prevent malicious attack	
14		The solution must have machine-learning based antivirus native to the solution	
15		The solution must have built in maintenance tool developed by the manufacturer of the video management.	
16	Safety approvals	The server must hold CSA or UL Listed Safety Approval	
17	Throughput	Minimum Validated throughput from Video management software provider of 650 Mbps with Min recording throughput of up to 500 Mbps and live rerouting traffic throughput of Min 150 Mbps and playback of 20 Mbps.	
18	Warranty	5 years NBD KYHD warranty support	

8) SPECIFICATION OF WORKSTATION FOR OPERATOR:

SL. No	Specification	Compliance (yes/ No)
1	Work Station PC with Core i7/ Ryzen 7 Processor, 32GB RAM, 512GB SSD, 1TB HDD, 8 GB Graphics Card, 1400-Watt Power Supply, Microsoft Windows 11 Professional License, Key Board & Mouse.	

9) SPECIFICATION OF IP SPEAKER/HORN

SL.No	IP PA Speaker System Specification	Compliance (yes/ No)
1.0	Low profile High SPL all weather loudspeakers with 5.25" LF Driver & 1.0" or better VC compression driver; Frequency Range of 100 Hz - 16 kHz or better; Nominal Dispersion: 90°H x 60°V with rotatable horn; Long term Power handling of 200 W or better; Sensitivity: 91 dB; Min SPL: 110dB Peak; Nominal Impedance 8 ohm; 18-gauge (1.2 mm) perforated steel; Powder-coated finish grille with Two-part spray polyurethane coating Enclosure. Shall include In-box 100W OEM Input transformer kit for distributed system applications. Shall	Nos

	be rated for IP55 outdoor installations as per IEC 529 specs.	
3.0	8 channel class D Networkable Power amplifier with a Max Output Power of 8x500W@8 ohms, or bridged mode output power of 4x 1000W @ 8/4 ohms. 20Hz - 20 KHz, SNR of 102dB and THD" N of <0.4% with built in protection such as Limiters, Temperature, DC, Short Circuit, Peak Current Limiters, Turn on delay etc. Built in DSP for Matrix routing, Speaker equalization, Delays, Array EQs etc complete with Ethernet Port for Network Control, programming and monitoring. Shall offer optional Network audio connectivity (Dante or CobraNet) through expansion slot.	Nos
4.0	Digital Signal Processor with at least 12 AEC Mic/Line inputs & 8 analogue outputs, 24 Bit A-D and D-A Convertors; Sampling Rate : 48 kHz; THD : « 0.002 % ; Channel Separation (Crosstalk) : < 108 dB ; Frequency Response 20 Hz - 20 kHz ; Signal-to-Noise Ratio 90 dB ;Dynamic Range » 115 dB; 5 Control Inputs and Outputs; RS-232 and Ethernet Port for third party Control and Monitoring; 64x64 Bidirectional DANTE Audio Networking ports, Shall include standard Connectivity features like VOIP, POTS, USB Audio etc. inbuilt DSP features like Conference room Routers, Input Equalizers, Router, Band Pass filter, Output Equalizer, Delay, Limiters, gates , Source selectors etc. Shall Support at least 15 remote Zone controllers.	Nos

10) SPECIFICATION OF LAYER-3 SWITCH

Layer 3 Managed Switch with 24 Port SFP + 2x40G QSFP+ Ports			
Sl. No	**Specification Required**		**Compliance (Yes/No)**
1	Type of Switch	Non-PoE Layer 3 Switch with full IPv6 support along with IPV4 & Dual Stack configurable.	
2	Port Density	a. 10G SFP+: At least 20 Nos. (but should meet the requirement)	
3		b. 1000 BaseT (RJ45): At least 04 Nos RJ45 Port	
4		c. 40G At least 2 Nos QSFP Port.	
5	Switching capacity	360 Gbps or better, non-blocking	
6	Stacking bandwidth/MC-LAG/Multi-Chassis Trunking (MCT)	40 Gbps or better	
7	Forwarding performance	260 Mpps or better	
8	Supported Power supply Options	AC+AC, AC+DC, DC+DC however Dual AC supply to be consider for BOM preparation.	

9	Console Port	Available	
10	MAC Address Table Size	minimum. 32000 entries	
11	Operating Temperature Range (Degree C)	'-20ºC to +65ºC (or better)	
12	Operating Humidity (RH %)	10% to 90% (non-condensing)	
13	Cooling fan	3+1	
14	Dedicated Stacking (port/Slot) or MC-LAG capability	min. 2 Nos	
15	Features	a) Supports 9 KB Jumbo frames.	
16		b) 1000 Active VLANs (802.1Q), VLAN tagging.	
17		c) Supports at least 8 MSTP Groups/Instances.	
18		d) IEEE (802.1D) STP, RSTP(802.1w), MSTP (802.1s).	
19		e) IEEE 802.3ad LACP- Link Aggregation.	
20		f) IEEE 802.1AB LLDP.	
21		g) Static Routing and Dynamic Routing (RIP v1 & v2 Present) from Day 1 with 32K Routes	
22		h) Support OSPF, VRRP, ECMP,BGP from Day1	
23		i) Support for Multicast, ,IGMPV1/V2, IGMP V3 Snooping.	
24		j) IEEE 802.1p prioritization, DiffServ/COS.	
25		k) Broadcast and Multicast Suppression.	
26		l) ACLs/filters.	
27		m) Support for Rate limiting/Queue Shaping.	
28		p) DHCP Snooping, DHCP Relay for IPv4 and IPv6 (RFC- 3315).	
29	Management	a) Console Management Port on the front panel.	
30		b) SMMP V1,V2 and V3 Support.	
31		c) SSH V2 Support.	
32		d) Telnet Support, TFTP.	
33		e) Port Mirroring.	
34		f) Industry Standard CLI with built in Scripting tool.	
35	Quality of	a) IEEE 802.1p Priority.	

36	Service	b) Diff. Serv Marking /Classification, Diff Serv	
37		c) 8 Nos. QOS Queues per Port	
38		d) IPv6 traffic identification, prioritization, redirection.	
39	Security Feature	a) 802.1x port based network access control & Authentication Protocols.	
40		b) RADIUS / TACACS+ Authentication support	
41		c) MAC Based Port limiting	
42		d) SSH Remote Login	
43		e) ACLs	
44		f) SNMPV3	
45	Form Factor	Rack Mountable	
46	Installation	Complete installation/ configuration with supply of suitable mountings, power supply/power injector/power adapter/ power cable/ patch cords and other accessories as required.	

11) SPECIFICATIONS LAYER-2 – 24 PORT POE SWITCH WITH 4X 1G SFP PORT

PoE+ Access Switch-with 24 x 10/100/1000M BASE-T RJ45 Port & 4 x 1/10G SFP/SFP+ Ports		
Sl. No	**Specification Required**	**Compliance (Yes / No)**
1.0	Product details- Please specify	
1.1	Please mention Make, Model No. and Part Code	
2.0	Architecture & Port Density	
2.1	Switch should offer Wire-Speed Non-Blocking Switching Performance at Layer 3 Access Switch.	
2.2	PoE Switch should have Twenty Four (24) 10/100/1000 Base-T RJ45 ports and Four (4) 1/10GbE SFP/SFP+ Ports	
2.3	Switch should support PoE/PoE+ on all 24 Port.	
2.4	Switch Should have min 370W PoE Budget.	
3.0	Performance	
3.1	Switching Bandwidth: Should provide Non-Blocking switch fabric capacity of 128Gbps or more.	
3.2	Forwarding Capacity: Should provide wire-speed packet forwarding of 95 Mpps or more.	
3.3	Layer 2 Switch with full IPv6 support along with IPv4 & IPv6 Dual Stack configurable.	
3.4	The switch should have Minimum 1GB RAM and 128MB Flash.	
4.0	Layer 2 features	
4.1	Switch should support 4K VLANs and 802.1Q VLAN tagging.	
4.2	Switch should support 32K MAC addresses or more.	
4.3	Switch should support IP multicast snooping with support for IGMP v1, v2, v3 and MLD v1/v2.	

4.4	Switch should support Jumbo Frames (up to 9K bytes)	
4.5	The switch should support Minimum Following IEEE Protocol: (802.1D) STP, RSTP (802.1w), MSTP (802.1s), IEEE 802.3ad LACP- Link Aggregation and IEEE 802.1AB LLDP.	
4.6	The Switch should support ACLs/filters, Support for Rate limiting/ Queue Shaping, Dynamic VLAN Assignment, DHCP Client, NTP (IPv4 and IPv6), Configuration backup and restoration, Port Mirroring, Private VLAN	
5.0	Layer 3 features	
5.1	Switch should support Basic IPv4 and IPv6 Static Routing.	
5.2	Switch Should support Inter-VLAN Routing from Day one.	
5.3	Switch should have Advance Dynamic Routing protocol (OSPF v2/v3 and RIP v1/v2)	
5.4	Switch should have Minimum 16K IPv4 Route and 8K IPv6 Route.	
6.0	QoS and Security	
6.1	Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords.	
6.2	Switch should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
6.3	Switch should support IP Source Guard, DHCP snooping and Dynamic ARP Inspection.	
6.4	Switch should have Minimum 3K ACL support for IPv4 and IPv6.	
6.5	Switch should support Byte and packet based broadcast, multicast, and unknown-unicast limits with suppression port dampening.	
6.6	Switch should support IPv6 Router Advertisement (RA) Guard.	
6.7	Switch should support Flexible Authentication with 802.1x Authentication and MAC Authentication.	
6.8	Switch should IEEE 802.1p Priority, 8 Nos. QoS Queues per Port, Shaping and Policing and DiffServ Marking/ TOS/ Classification.	
7.0	Manageability	
7.1	Switch should support manageability using Network Management Software with Graphical User Interface (GUI), it also support web Based Management through EMS/NMS/Switch based HTTP Host.	
7.2	Switch should provide Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP /HTTPS access to switch management/monitoring	
7.3	Switch should support following File Transfer Protocols: SCP, TFTP.	
7.4	The Switch should have Industry Standard CLI.	

8.0	Physical Attributes, Power Supply, temperature and Humadity Details	
8.1	Mounting Option: 19” Universal rack mount ears	
8.2	Minimum 1.5 Meter Indian Standard Power cable/cord.	
8.3	The Switch should support Operating Temperature Range (Degree C): 0ºC to +50ºC	
8.4	The Switch should support Operating Humidity (RH) (%) : 5% to 95% (non-condensing)	
8.5	The Switch should supplied with Integrated AC Power Supply (100V - 240V AC) and Minimum 1.5 Meter Indian Standard Power cable/cord.	
9.0	Warranty and brochure	
9.1	The switch, including 24/7 phone, email, and chat support from your TAC team, along with 5-year warranty covering hardware and Software replacement.	
9.2	The Switch Should not be Bound to any License for any feature; the entire asked feature set should be available from day one.	
9.3	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications and features.	

12) SPECIFICATIONS LAYER-2 - 8 PORT POE SWITCH WITH 2X 1G SFP PORT

8 Port PoE/PoE+ Access Switch-with 8 x 10/100/1000M BASE-T RJ45 Port & 2x1G SFP + 2x1G RJ45 Uplinks,		
Sl. No.	**Technical specification**	**Compliance Yes/No**
1	Should have 8 ports 10/100/1000 Mbps Base T supported PoE/PoE+.	
2	Should have 128 MB RAM & 32 MB Flash from day 1.	
3	Should have for 2 ports SFP ports and 2x1G RJ45 Uplinks	
4	Should have at least 20 Gbps switching fabric.	
5	Should support at least 8K entries in the MAC table.	
6	Packet forwarding rates 14 million PPS	
7	Should Support 2048 minimum VLANs.	
8	The Switch should have minimum 120 Watt PoE Budget	
9	Should have AC Power Supply 100 to 240 V AC with 50 to 60 Hz and equipped with 3 pin plug.	
10	Should support Dual Images.	
11	Should support port mirroring and jumbo frame.	
12	Should support following for min. 64 Groups :	
	i) IGMP Snooping, MVRP	
	ii) IGMP v1/v2/v3 awareness Snooping,	
	iii) IGMP Snooping Queried.	
	iv) MLD Snooping	
13	Should support RSTP, spanning-tree root guard, Port Fast and	

	BPDU Guard/Filter or similar functionalities.	
14	Switch should support :	
	i) Surge protection of Min ± 1 kV (line-earth) and ± 1 kW (line-line) on power	
15	Should support following security features viz.:	
	i) Command Line Interface (CLI) and Web Management (HTTPS).	
	ii) Broadcast/Multicast/Unicast Storm Control,	
16	Switch should support following SNMP traps or Syslog	
	i) Interface UP & Down	
	ii) Optical power SFP threshold alarms	
	iii) STP Topology Changes and New root bridge	
	iv) LLDP table changes	
	v) Threshold alarms for Temperature.	
17	Switch should comply to following Temperature performance parameters :	
	i) Operating Temperature - min -5 to 50 °C (23 to 122 °F)	
	ii) Storage Temperature - min -0 to 70 °C (-40 to 158 °F)	
18	It should be IPv6 Compliant and should be capable of working on IPv6 without any additional hardware/software	
19	It shall support MAC address notification to allow administrators to be notified of users added to or removed from the network.	
20	The switch shall be designed for continuous operations.	
21	IPv6/v4-L3 and IPv6-Multicast functionalities/features for Switches are desired but not mandatory.	
22	The LAN switch shall support a console port or auxiliary/Ethernet port for the purpose of local and remote configuration and diagnostics.	
23	802.1x: Port security, Single and Multiple Authentications, MAB	

13) SPECIFICATIONS FOR 24U MDC RACK

Specification - 24U 800W 1000D RACK WITH 1000WATTS PANEL AC		
Sl. No.	**Technical specification**	**Compliance Yes/No**
1	System:	
1.1	Rack should be designed to provide Compatible, Secure, Monitored, Manageable, simplifying infrastructure deployment in Edge Environment.	
1.2	Rack should be self-Contained with proper air circulation.	
1.3	Rack should be designed so that it is compatible with latest converged and hyper-converged IT System.	
1.4	The Enclosure solution should be 24U 1305 mm (Overall) in height with 1060 mm Width and 1000 mm Depth for Server &	

	Networking application.	
1.5	Overall weight shall be maximum 170 Kgs, including enclosure, cooling unit with bracket and power distribution panel.	
1.6	Power supply input: Single Feed AC 230V +/-10% /1P/50-60Hz.	
1.7	IT Load: Shall not be more than 1000W	
1.8	Country of Origin: India	
2	Physical Requirement:	
2.1	The Rack should support a static load of 1000 kg.	
2.2	Doors: The Rack Front door shall have Glass panel and Rear Metal Plain split door.	
2.3	Doors shall be reversible with capability to install hinges on left or right position	
2.4	Mechanical swing handle with 3 point locking provision.	
2.5	The Rack should have one full side panels and panel ac provisioning on the other side panel. Top & Bottom, grounding and bonding accessories pre-installed by the OEM.	
2.6	Installation type: Floor mount	
2.7	The overall Rack height shall be inclusive of 100mm bottom plinth	
3	Equipment Access & Installation	
3.1	Space inside the cabinet to be suitably designed for optimum use of available space inside cabinet.The Rack should have minimum 24U available usable Space.	
3.2	The Rack should have 4 Nos. 19” verticals equipment mounting angles with 'U' marking, screen printed.	
3.3	The Rack shall include 4 M12 eyebolts and a side bracket as a provision to fix fire extinguisher.	
3.4	The front and rear doors should be easily detachable and openable for ease of accessing.	
4	Material Requirements	
4.1	19” equipment mounting angle should be 2MM.	
4.2	All sheet metal parts should be Pre Treated and powder coated.	
5	Certifications, Environmental and Safety Requirements	
5.1	Racks should be manufactured by ISO9001:2008, ISO14001:2004, ISO 45001:2018 & ISO 50001:2018 Certified company and should have proper EHS Policy.	
5.2	Manufacturing process shall comply with ROHS and REACH standards.	
5.3	The rack shall be IP54 certified from an accredited lab.	
5.4	Maximum Noise Level: ≤ 65 dBA at 1 meter	
6	Thermal Management	
6.1	The Rack shall include a pre-integrated Panel AC on the side of the rack	
6.2	The Rack shall include a bottom bracket support under the cooling unit for stability purposes	
6.3	The Panel AC Cooling unit shall have the following nominal cooling capacity (L35/L35) 1KW	

6.4	The cooling unit operative range shall be from 10ºC to 50ºC	
6.5	The cooling unit compressor shall be Rotary type in order to minimize vibration and noise level, suitable for IT applications.	
6.6	The internal condenser coil shall be based on hydrophilic aluminum fins with copper tubes	
6.7	The main refrigerant for the cooling unit shall be R134a	
6.8	The cooling shall include a smart controller with RS485 MODBUS interface as well as dry contacts.	
6.9	The cooling unit shall include High pressure Switch, Low pressure switch and an interface to connect a voltage sensor relay	
7	Cable Management	
7.1	The Rack shall have dedicated cable management space: 1 No. Side cable gland for power input with 4 separate entries. 2 Nos. Top Cable glands with capacity for 37 data cables 3 Nos. of Plates for cable gland addition (2 At Top & 1 At Side Bottom) 2 Nos. of Plates at the bottom panel for cable gland addition.	
8	Cabinet Interior Lightning:	
8.1	Front & back LED Lights to be provided.	
9	Remote Monitoring	
9.1	The cooling unit shall include a RS485 interface port The cooling monitoring system will be based on MODBUS serial protocol and will be enabled to provide the following information: Cooling State Internal Fan State External Fan State Dry Contact Alarming State Return Air Temp Sensor Fault High Pressure Alarm Low Pressure Alarm High Return Air Temperature Alarm Low Return Air Temperature Alarm External Digital Input Alarm Return Air Temperature FW version Serial Number Model name Compressor setting temperature Compressor tolerance temperature Cabinet inside high temperature limit Cabinet inside low temperature limit Internal fan state in standby mode	
10	Power subsystem:	
10.1	Vertical 0U power distribution panel which distributes the input feed in various feed for components connected to it with MCB's at each level.	
11	Delivery & Installation	

11.1	The unit should be shipped fully assembled as one orderable Unit including enclosure, Panel AC and power distribution panel	

14) SPECIFICATION OF OUTDOOR UTP CABLE

Sl. No.	Parameter	Specification	Compliance (Yes/No)
1	Type	Category 6 U/UTP ECCS Armored Cable	
2	Type	23 AWG solid bard Electrolytic Grade Copper Conductors, Unshielded Twisted 4 Pair, PVC, Electrolytic Chrome-coated Corrugated Steel Tape Armoring covered with PE Outer Sheath. Category 6, confirming to ANSI-TIA 568.2-D for Category 6 & ISO/IEC 11801 for Class E.	
3	Support	Supports Gigabit Ethernet (1000BaseT) standard requirement for Applications such as High-Speed Data, Voice & Video Signals over LANs, Server Farms and Other Bandwidth Sensitive Outdoor Applications.	
4	Conductors	Solid bare copper 23 AWG	
5	Pair Separator	+ Shape Spline	
6	Packing	Box of 305 meters	
7	Cable Outer Diameter	10.5 + 0.5 mm	
8	Outer Sheath	PE	
9	Outer Sheath Color	Black	
10	Delay Skew	< 45 ns	
11	Conductor Resistance	≤ 9.38 Ω /100 m	
12	Mutual Capacitance	<5.6nF/100m	
13	Resistance Unbalance	5% Max	
14	Capacitance Unbalance	330 pF/100 m	
15	Bend Radius	8 X Cable Diameter	
16	Pulling Force	25 lb	
17	Nom. Velocity of Propagation	69%	
18	Temperature Range Operation	-20 °C to +70 °C	
19	Temperature Range Installation	0 °C to +50 °C	
20	Maximum propagation delay @250MHz	490ns/90m	
21	Regulatory Compliances	Should be ETL channel performance verified on a	

		04-Connector channel or more, tested upto 350Mhz or more with an MTPL Plug as per ANSI/TIA-568.2-D (Part Code to be mentioned in report and should be submitted along with bid)	
		Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863 (Relevant Document to be enclosed along with Bid)	
		OEM should be a member of BICSI and should have a certified project management professional (PMI-PMP®) and a CDCP® / RCDD® on the OEM's payroll sitting in India whose services can be utilized for this project.	
		OEM should be an ISO9001, ISO 14001 and ISO 45001 should have its Manufacturing units, Components and Finished Goods Warehouse & R&D labs in India. (Relevant Document to be enclosed along with Bid)	
22	Test Reports	OEM factory test reports must be provided.	
23	Make & Model	Bidder to specify	

15) SPECIFICATIONS 6 CORE FIBER OPTIC CABLE

Sl. No.	Parameter	Specification	Compliance (Yes/No)
1	**Type**	6/12F Core Single mode (9/125µm) Multi loose Tube, Double Sheath, G652.D Fiber cable is perfectly suited for both gigabit Ethernet and 10 gigabit Ethernet campus and backbone applications	
2	**Cable**	6/12 Core Single mode, Multi loose tube with colored fiber cores. The constructions are of excellent water proof layer and good moister resistance.	

3	**Application**	This cable is suitable for direct burial applications. Cable are perfectly suited for both gigabit Ethernet and 10 gigabit Ethernet campus and backbone applications.	
4	**Outer & Inner Sheath**	HDPE Jacket / Black	
5	**No. of Tube / Tube diameter**	1/4 or 2/3 : PBT having diameter 1.8 ± 0.1 mm	
6	**Water Blocking Material**	WS Tape	
7	**Loose Tube Construction**	Std. plywood reel: Uni loose Tube, Yarn / Tape with fibers. Individually color coded optical fibers as per Global Standards	
8	**Cable Specifications**	Fiber Color / Fibers per Tube : Blue, Orange, Green, Brown, Grey, White, Red, Black, Yellow, Violet, Pink, Aqua	
		Cable diameter : 13.5 ± 0.5 mm	
9	**Central Strength Member**	FRP	
10	**Armouring**	ECCS Tape Armoured below each Jacket	
11	**Optical Properties**	Core Non-circularity : ≤ 6 %	
		Cladding Diameter : 125.0 ± 0.7 µm	
		Core/cladding Concentricity Error : ≤ 0.6µm	
		Cladding Non-circularity : ≤ 1.0 %	
		Primary Coating Diameter : 245±10µm	
		Coating/cladding Concentricity Error : ≤ 12µm	
		Attenuation Co-efficient (After Cabling)	
		1310 Wavelength (nm) : ≤0.36 dB/km	
		1550 Wavelength (nm) : ≤0.22 dB/km	
		Chromatic dispersion :	
		1285 ~ 1330nm ≤ 3.4ps/(nm·km)	
		1550nm ≤18 ps/(nm·km)	
		1625nm ≤ 22 ps/(nm·km)	
		Cutoff Wavelength ≤ 1260 nm	
		PMDQ (Quadrature average*) : ≤ 0.20 ps//km½	
		MFD : 9.0 ± 0.4 µm at 1310nm	
		Zero dispersion slope : ≤ 0.092ps/(nm2·km)	
		Zero dispersion wavelength : 1302~1324nm	
12	**Temperature Range**	Storage Temperature Range: -40°C to +70°C	
		Installation Temperature Range: -40°C to +60°C	
		Operating Temperature Range: -40°C to +70 °C	

13	**Physical Properties**	Complies to ANSI/TIA-568.3-D, ITU-T G652.D, Telcordia GR-20, IEC 60794-2, ISO/IEC 11801,ISO/IEC 24702	
		Cable Bend Radius : 30 x Cable Diam.	
		Cable Kink Radius : 10 x Cable Diam.	
		Cable Max. Tensile Strength (Short Term) : 4000 N	
		Cable Max. Crush Resistance (Short Term) : 4000 N / 100mm	
		Impact Resistance : 25 Nm	
14	**Regulatory Compliances**	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863 and the OEM shall be a Class 1 local supplier as defined in public procurement (Preference to Make in India), .	
		The OEM should be CE Certified and its manufacturing facility must adhere to Environmental Management Systems (EMS) through ISO 14001:2015 and adhere to Occupational Health and Safety (OH&S) management system through ISO 45001:2018 (Certificates to be Enclosed)	
		The OEM shall be recognized by the Department for Promotion of Industry and Internal Trade under the 'Telecommunication & Networking' Industry and 'Network Technology Solutions' sector by Government of India.	
		OEM offered must be in India / SAARC for at-least 10 years or more. Should have Indian Technical Support Centre, Warehouse and RMA centre in India.	
15	**Test Reports**	OEM factory test reports must be provided against each drum / roll of fiber cable.	

16) SPECIFICATIONS OF FIBER RACKMOUNT LIU LOADED TYPE 12/24 PORT

SITC of 12F / 24F, 1U Rack Mount Fiber Enclosure (LIU) including Splice Trays and Adapter Strips having minimum technical specification as mentioned below:			
Sl. No.	**Parameter**	**Specification**	**Compliance (Yes/No)**
1	Type	1U, 19 Inch Rack Mount Fiber Enclosure (LIU) including Splice Trays and Adapter Strips which accepts loose tube & distribution cable	

2	Fiber Interface Unit	Fiber Patch Panel Typically used in Server rooms, Network rooms, Data Centers and Small Offices Can be mounted directly on any 19" rack or cabinet. It should be able to accommodate a variety of Fiber connectors and terminated to fiber cables using Splicing or other methods.	
3	Features & Compatibility	The Fiber Panels are designed with fixed mount adapter plate assemblies. Should be available in 6 - 96 Port in 1U Rack Mount LIU.	
		Sliding design, this panel allows easy access during installation or rework without disturbing previously terminated fiber cable.	
		This also offers multiple cable entries to provide various customized solutions as per the customers' requirement.	
		This panel comes with adaptor plates which are preloaded with coupler and can snap in for installation and can be removed easily for future changes.	
		900m Tight buffer pigtails are provided with this panel. This panel is preloaded with Splice tray & necessary fiber management accessories.	
		4 Nos of 20mm diameter at the rear for Cable entries.	
4	Material	Panel be constructed with SPCC (Cold rolled steel sheet)	
5	Standards	Conformance to Single Mode (ANSI/TIA-568.3-D, Telcordia GR-326-CORE, Telcordia GR-1221-CORE, ISO/IEC 11801, IEC 61754 & IEC 61300 series).	
6	Adapter Types	Pigtails consist of LC, SC, FC, ST, MTRJ, and E2000 Connectors.	
7	Pigtails Type	Pigtails shall be constructure with bend Insensitive Fiber	
8	Insertion Loss	≤0.2 dB (Single mode)	
9	Return Loss	≥50 dB (UPC), (Single mode) , ≥60 dB (APC) (Single mode)	
10	Repeatability	≤0.1dB	
11	Durability	≤0.2 dB, 1000mattings	
12	Ferrule Material	Zirconia Ceramic	
13	Operating Temperature	-25 °C to +70 °C	
14	Regulatory Compliances	Compliant as per RoHS Directive 2011/65/EU and (EU) 2015/863	

		OEM should be an ISO9001, ISO 14001 and ISO 45001 should have its Manufacturing units, Components and Finished Goods Warehouse in India. All Related documents to be submitted.	
		The Proposed OEM should be a member of BICSI and should have a CDCP and a PMI-PMP / RCDD on the OEM's payroll sitting in India whose services can be utilized for this project.	
		OEM offered must be in India / SAARC for at-least 10 years or more. Should have Indian Technical Support Centre, Warehouse and RMA centre in India.	
15	Make & Model	Bidder to specify	

17) SPECIFICATION OF ON-LINE UPS-1 KVA

1 KVA Line Interactive UPS Specification			
SL.No	**Parameter**	**Specifications**	**Compliance (yes/ No)**
1	Capacity	1000VA/600W	
2	Input Voltage Range	140 V ~ 300 VAC	
3	Frequency	50 Hz ± 10%	
4	Output Voltage	230 VAC Nominal	
5	Transfer Time	Typical 4~8ms	
6	Waveform (Battery Mode)	Modified Sine Wave	
7	Battery Type	Sealed Maintenance Free	
8	Charging Time	6~8 Hours recover to 90% capacity	
9	Battery Rating	SMF 12V /7AH x 2 Battery	
10	Operating Temperature	0°C-40°C;	
11	Relative Humidity	0 to 90% non-condensing	
12	Noise Level	< 40dB	

18) SPECIFICATIONS FOR ON-LINE UPS -10KVA

10 KVA Online UPS Technical Specifications			
SL.No	**Parameter**	**Specifications**	**Compliance (yes/ No)**
1	Input		
1.1	Nominal voltage	200/208/210/220/230/240VAC	
1.2	Voltage range	110-300VAC(at 50%load) or 176-300VAC(at 100% load)	
1.3	Frequency range	46-54Hz	
1.4	Power factor	>=0.99 at nominal	

		voltage(100%load)	
2	Output		
2.1	Voltage regulation	+/- 1%	
2.2	Output voltage	200/208/210/220/230/240VAC	
2.3	Frequency range(synchronized range)	46-54Hz	
2.4	Frequency range (batt. Mode)	50+/- 0.1%	
2.5	current crest ratio	3:01:00 AM	
2.6	Harmonics distortion	<= 3% THD(linear load) <=5% THD(nonlinear load)	
2.7	Waveform (battery mode	pure sinewave	
2.8	Overload	105-110%: 10 mins,110-130%:1 min,>130%: 3 sec	
3	Efficiency	93%	
4	Battery		
4.1	Numbers	16 or 20	
4.2	Charging current Max	1A/2A/4A(Adjustable,4A is only available)	
4.3	Additional charger	8A	
5	Indicators		
5.1	LCD	Load level, battery level, AC mode, battery mode, bypass mode and fault indicators	
6	Physical		
6.1	Dimension DxWXH MM	400x195x335	
6.2	Net weight	16	
7	Humidity	20-90%RH @0-40 degree C (non-condensing)	
8	Noise level	Less than 58DB @1 meter	
9	Management		
9.1	Smart RS -232/USB	support windows 2000/2003/XP/Vista/2008,windows 7/8,Linux and Mac	
9.2	Optional RS 485	SNMP, Modbus (RS 485) and potential free contact	

19) SPECIFICATION OF SPD- (SURGE PROTECTION DEVICE)

SL .No	Parameter	Specifications	Compliance (Yes/No)
1	Nominal voltage	48V	
2	MCOV	64V	
3	Load current	1.5A	
4	Frequency	250MHz	
5	Impulse current rating(10/350µS)	1kA	

6	Nominal discharge current(8/20µS), C2	3kA	
7	Total discharge current(8/20µS)	20kA	
8	Voltage protection level	<100V @ 3kA	
9	Insertion loss	<1dB @ 250MHz	
10	POE Compliance	Type 1&2 according to IEEE802.3af,at and Type3&4 POE according to IEEE802.3bt	
11	Mounting	DIN rail and surface mount	
12	Connection cable	STP and UTP cable	
12	Ambient temperature	-40Deg C to +75Deg C	
13	Compliance	Design comply to ANSI/TIA568.2-D, TIA/EIA-568- B.2-1, IEC61643-21. Testing in progress	
14	Certification	Tec	

2.4 Other Requirements

a. The solution must have centralized applications and database.

b. All the CCTV Camera should be visible from the central console. The console should indicate the status of every CCTV Cameras with latest images/footages.

c. The solution should have the capability to integrate with other surveillance systems of different brands with the objective of enhancing safety & security in the Arilo Dairy Campus & Other Units wherever applicable.

d. OMFED will provide the necessary infrastructure support for device installation at the specified locations and to connect through OMFED intranet and internet.

e. At the respective sites, OMFED will provide the space for mounting the devices.

3. Delivery period and Milestone

The vendor shall complete the Implementation and configuration of the CCTV Surveillance System as well as achieve "Go-Live" for Arilo Dairy, OMFED within a timeframe as mentioned below from the date of issue of LoA.

Sl. No.	Milestone	Time for Completion (in Weeks)
1.	Project Start (Signing of Agreement)	T= Date of Agreement
2.	H/W Installation	T+6
3.	System testing and validation	T+8
4.	Go-Live of CCTV in Arilo Dairy	T+12

Note – The above schedule is indicative. The detailed time schedule for Arilo Dairy, OMFED shall be finalized in joint consultation between the Vendor and OMFED. However, the overall

timeline of achievement of "Go-Live" for CCTV Surveillance System as mentioned above shall remain fixed.

4. Payment terms

4.1 The place of payment shall be Head Office, OMFED. Invoices shall be placed to, IT Division for verification & processing.

4.2 **Payment Schedule**

4.2.1 **Charges for AS IS Process, Hardware Supply, Configuration of Hardware and Software Installation and Go Live.**

Sl. No.	Milestone	Payment
1.	Hardware Supply / Materials Delivery	70% Charges with Applicable GST
2.	Configuration of Hardware & Software, Installation, Commissioning, Testing, Go-Live	Rest 30% with Applicable GST

4.2.2 **Annual AMC of CCTV at Arilo Dairy, Cuttack**

Sl. No.	Milestone	Payment
1.	Completion of each quarter successful report of AMC Support for CCTV at Arilo Dairy, Cuttack is required for renewal of AMC for next Year.	25% of Annual Charges with applicable GST on successful completion of each quarter.

5. Service level agreements (SLA) during AMC Period

The installed system should have an uptime of 99.0 % up time. In case of uptime falls below 85%, the contract shall be liable for termination.

6. Price Revision

No price revision shall be applicable throughout the Delivery Period and the contract period. 5 years' same rate contract for future enhancement for OMFED.

7. Taxes & Duties

7.1 Indirect Taxes

A) The Service Provider agrees to and, hereby accepts full and exclusive liability for payment of any and all taxes, duties, charges and levies as per the Applicable Laws as applicable for the Scope of Supply in accordance with the provisions of this Service Order / Agreement. In case it is increased or decreased under any statute, rules, regulations, notifications, etc. of any Authority, the impact shall be to the account of OMFED subject to submission of documentary evidence to the satisfaction of OMFED.

B) In case any fresh tax is imposed by any Authority under any Applicable Law during the Contract Period, the Service Provider shall deposit the same to the appropriate Authority which shall be reimbursed by OMFED on actuals and upon submission of documents

evidencing such payment.

C) Obligations relating to Goods and Services Tax (GST)

i. The Service Provider should have registration under GST Acts.

ii. The Service Provider has to raise Invoice as required under section 31 of the GST Act and relevant Rules made there under.

iii. The Invoice should contain the particulars as required under Rule 46 of CGST Rules.

iv. The Service Provider should file the GST Returns as required in the GST Acts, and details of Invoice submitted to OMFED and GST amount charged thereon should reflect in Form GSTR-2B within a reasonable time, so as to make OMFED enable to take Input Tax Credit (ITC) of the GST amount paid against those invoices.

v. If due to any reason attributable to the Service Provider, input credit of the GST amount paid on Invoices raised by the Service Provider is not available to OMFED/denied by the department then the same will be recovered from the payments of the Service Provider or the Service Provider has to deposit an equivalent amount.

vi. The Service Provider has to comply with all the Provisions of GST Acts, Rules and Notifications issued there under.

vii. The Service Provider will comply with the “Anti profiteering Measure” as required under Section 171 of the CGST Act.

viii. The Service Provider hereby undertakes to indemnify OMFED, from any liabilities arising in future due to noncompliance by the Service Provider of the GST Acts, Rules and any other Acts currently in force and applicable to the Service Provider in relation to the job assigned to the Service Provider by OMFED.

ix. TDS as applicable under GST Act shall be deducted from the bills by OMFED.

7.2 Direct Taxes

TDS as applicable shall be deducted under Income Tax Act,1961 and certificate of deduction shall be provided by OMFED to the Service Provider in accordance with the provisions of Income Tax Act,1961.

8. Liquidated Damages

8.1 If the Service Provider fails to achieve the Go-Live of the CCTV Surveillance System within the corresponding Delivery Period and any extension thereof, unless such, unless such failure is due to force majeure situation or due to OMFED's default, liquidated damages (LD) shall be imposed by OMFED on the Service Provider. However, imposition of LD shall be without prejudice to the other remedies available to OMFED under the terms of the Service Order / Agreement.

8.2 In case of delay in achievement of Go-Live of the CCTV Surveillance System, the LD shall be calculated as 2% (two per cent) of the total value of CCTV Surveillance System (excluding GST) for each month or part thereof of delay, subject to a maximum value of 10% of the value of CCTV Surveillance System (excluding GST). GST on LD shall be recovered in addition to the LD amount.

8.3 The delivery period shall start from the date of acceptance of the Service Order / Agreement or seven days from the date of issue of Service Order / Agreement, whichever is earlier.

8.4 OMFED shall have full liberty to realize the LD through the following ways:

a. Appropriation of the Performance Security; OR

b. Appropriation the of EMD (in case provision of Performance Security does not exist); OR

c. Reduction of the invoice/document value and release of the payment accordingly.

8.5 Any waiver of LD shall be at the sole option of OMFED only and any extension must be in writing and with the approval of the competent authority of OMFED.

8.6 If at any time during the Service Order / Agreement, the Service Provider encounters conditions that may impact the timely performance of services, the Service Provider shall promptly notify to OMFED in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable after receipt of the Service Provider's notice, OMFED shall evaluate the situation and may at its discretion waive the LD on the request of the Service Provider.

9. Others

The vendor shall carry out all support related services for the UCC Platform based CCTV Surveillance System on a real-time basis for a period of 05 (Five) years as part of warranty starting from the date of achievement of "Go-Live".

Annexure 2A: Proforma of the Agreement to be Signed between OMFED and the Service Provider

(to be executed on INR 100 non judicial stamp paper and to be duly notarized)

Ref: [_____]

This Agreement (hereinafter called the "Agreement") is made on this [_] day of the month of [month], [year].

BETWEEN

The Orissa State Cooperative Milk Producers' Federation Limited and having its head office at D-2, Saheed Nagar, Bhubaneswar-751007 (hereinafter referred to as "OMFED", which expression shall, unless repugnant to or inconsistent with the context, mean and include its successors and assigns) of the first part.

AND

M/s. [_____], a company incorporated under the provisions of the Companies Act, 1956/2013 or a registered partnership firm under the provisions of the Indian Partnership Act, 1932 or a LLP firm registered under LLP Act, 2008 and having its registered office at [_____] (hereinafter referred to as the "Service Provider" which expression shall unless repugnant to or inconsistent with the context, mean and include its successors and assigns) of the other part.

WHEREAS

i) the Service Provider, in the ordinary course of its business, is engaged in providing [___] services to its clients, and have represented to OMFED through their bid(s), against Bid Document No. [__] dated [_/_/_] (hereinafter called the "Tender") for the Procurement of Services – [_____];

ii) on the basis of the said Tender, OMFED has adjudged the Service Provider as a successful Bidder and issued Letter of Award (LoA) No. [_____] dated [__/ /_] for the same;

iii) the Service Provider has agreed through their letter of acknowledgement vide letter No. [_____] dated [_/_/_] to perform and undertake the scope of work as described in the Tender;

iv) the Service Provider is being engaged to provide the required services on the terms and conditions set forth in this Agreement;

NOW THEREFORE THE PARTIES hereby agree as follows:

1. The mutual rights and obligations of the Service Provider and OMFED shall be as set forth in this Agreement, in particular:

(a) The Service Provider shall provide out the services in accordance with the provisions of this Agreement; and

(b) OMFED shall make payments to the Service Provider in accordance with the provisions of this Agreement.

2. Conditions of Contract

(a) Contract Period: <include relevant clauses from SCC>
(b) Payment Terms: <include details related to the final quoted /negotiated prices>
(c) <Other important terms and conditions may be included>
(d) The Agreement shall be governed by the laws of India and the courts of Bhubaneswar shall have exclusive jurisdiction over all disputes arising under, pursuant to and/or in connection with this Agreement
(e) This Agreement has been executed in English, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Agreement
(f) All the terms and conditions as per the Bid Document No. [___] dated [__/__/__] (including the General Conditions of Contract and Special Conditions of Contract) shall be applicable for this Agreement

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their respective authorized representatives on the day and year first before written.

For and on behalf of OMFED (Authorized Representative) Name: Designation: OMFED D-2, Saheed Nagar, Bhubaneswar-751007	For and on behalf of M/s. (Authorized Signatory) Name: Designation: Name of the Service Provider: Address:

In presence of the following witnesses

Name: Designation: OMFED D-2, Saheed Nagar, Bhubaneswar-751007	Name: Designation: Name of the Service Provider: Address:

Annexure 2B: Undertaking from OEM on Authorization of Use of Their Products

(Company letterhead)

[Date]

To

The Managing Director,
OMFED
Bhubaneswar

Sub: Authorization of <company name of SI> to Provide Services Based on Our Product(s)

Sir,

This is to certify that I/We am /are the Original Equipment Manufacturer in respect of the products listed below. I/We confirm that <name of SI> ("SI") have due authorization from us to provide services, to OMFED, that are based on our product(s) listed below as per Request for Proposal (RFP) document relating to providing of the solution, Implementation, training & maintenance services, Information Technology Infrastructure and System Integration services to OMFED. We further endorse the warranty, contracting and licensing terms provided by SI to OMFED.

Sr No	Product Name	Remarks
1.		
2.		
3.		

Yours faithfully,

Authorized Signatory
Designation
OEM's company name

CC: SI's corporate name

Annexure 2C: Work Experience

LIST OF SIMILAR NATURE OF PROJECTS EXECUTED

Name of Dept / Organization	Name of location and name of work	Contract price in Indian Rupees/ Agreement no.	Major Items of works	Stipulated date of commencement	Date of completion of the work	Value of work actually executed during last 5 financial years		Reasons for delay in starting/ completion, if any
						Financial year	Value	
1	2	3	4	5	6	7	8	9

Note: The above information is to be self-attested and supported by copy work order / agreement, completion certificate and performance certificate issued by concerned authority. The above information, if found incorrect the bid shall be summerly rejected.

Signature of the Bidder
Date.

Annexure 3: Price Bid Format

Sl. No.	Items	Quantity	UOM	Unit Price in figures (₹)	GST %	Unit Price after GST (3+4) (₹)	Total Price (1*5) (₹)
		1	2	3	4	5	6
1.	Management Server with Microsoft server 2022 std. license	1	Nos				
2.	Primary NAS Storage 12 Bay, 8 nos. X 12 TB HDD with redundant power supply	1	Nos				
3.	Workstation with Core i7 12th Generation, 32 GB RAM, 6 GB Graphics card & windows 11 Professional	2	Nos				
4.	21.5'' Monitor Full HD	2	Nos				
5.	Core Switch -L3 24 Port Switch Fully Managed with 16 Copper + 8 SFP Ethernet Port	1	Nos				
6.	L2 Fully Managed 8 Port Giga PoE Switch PoE Output with 2 SFP Port.	19	Nos				
7.	IP 5 MP dome Camera POE Supported UL Certified with mounting accessories	50	Nos				
8.	IP 5 MP Bullet Camera motorised varifocal Lense POE Supported UL Certified with mounting accessories	10	Nos				
9.	4MP IP PTZ camera IR 200 mrt motorised varifocal Lense POE Supported UL Certified with mounting accessories	3	Nos				
10.	ANPR/ALPR camera- Edge based AI ML camera UL Certified with Industrial Grade Giga POE++ Injector and mounting accessories	2	Nos				
11.	12 port LIU with loaded	20	No				
12.	SC-LC Patch Cord	42	Nos				
13.	1000 Base 1310nm SM Transceiver Module	42	Nos				
14.	Cat 6 factory made patch cord 3 Mtr	20	Nos				
15.	Cat 6 double jacketed UTP Outdoor Cables	5	Box				
16.	Optical fibre cable -6 core, Single Mode, Armoured	500	mtrs				
17.	CCTV Dual/Triple Cantilever Galvanized Pole, Civil Foundation with Proper Chemical Earthing	3	Nos				
18.	Water & Dust proof Camera Back box	70	Nos				
19.	1 KVA UPS Internal Battery	19	Nos				

	Cables etc.						
20.	10 KVA Online UPS with External Battery Rack, Cables etc.	2	Nos				
21.	65" 4K HDR Professional Display with mounting accessories	2	Nos				
22.	98" 4K HDR Professional Display with mounting accessories	1	Nos				
23.	Micro Data Center, with 24U Indoor rack, 1 kW Panel AC cooling, 230V, 50/60 Hz, 1300H x 1060W x	1	Nos				
24.	RJ 45 Connector industrial Grade	2	pkt				
25.	Outdoor IP Horn/Speaker for PA system with all Accessories	5	Nos				
26.	Electric power cable with Field Location Electrical Work-All type(Approx.)	1	Lot				
27.	SPD (Surge Protection Device) Unit	20	Nos				
UNIFIED COMMAND & CONTROL SOFTWARE							
28	Unified command and control software with Video management software (VMS), GIS engine, PA (Public announcement application, Parking management application plugin, Realtime alert/ alarm, threat level & management Engine, Mobile & Web applications with UL certification	1	Nos				
29	Camera connection Licence with Advantage 5 Year support service	63	Nos				
30	ANPR/ALPR Camera Connection Licence with Advantage 5 Year support service	2	Nos				
31	PA system -IP horn connection license with Advantage 5 Year support service	5	Nos				
Service							
32	6 U Rack with all accessories installation	19	Nos				
33	OFC - 6 Core SM-Type Armoured cable with Laying, Termination accessories	4000	Mtr				
34	Cat 6 UTP Cables Indoor with laying pvc pipe	3660	Mtr				

35	Site Survey, Planning, Designing, Civil Work, Installation, Commissioning, Testing & Training of the complete system	1	Lot				
Annual Maintenance Charges Post Warranty							
Sl. No.	**Particulars**	**Quantity**	**UOM**	**Basic Rate (₹)**	**GST % (₹)**		**Total (Basic + GST) (₹)**
28.	AMC Charges for 1st Year post Warranty	01	Job				
29.	AMC Charges for 2nd Year post Warranty	01	Job				
30.	AMC Charges for 3rd Year post Warranty	01	Job				
31.	AMC Charges for 4th Year post Warranty	01	Job				
32.	AMC Charges for 5th Year post Warranty	01	Job				
	GRAND TOTAL						

Note: Grand total of Sl. 1-35 shall be considered for the decision of L-1 bidder, however OMFED can negotiate the prices mentioned in above tables by the bidder. (AMC value cannot be less than 10% for each year of total material cost for fair price bid.)

Signature of the Bidder with seal

Annexure 4: Declaration by the Bidder

(to be executed on INR 100 non judicial stamp paper and to be duly notarized)

Date:_____

Sub: Tender No. _____

In response to the Tender Document above stated, I/We hereby declare and solemnly swear that our Company/ firm _____ is not banned/blacklisted as on date by any competent court of Law, forum or any State Government or Central Government or their agencies or by any statutory entities or any PSUs.

AND, if at any stage the declaration/statement on oath is found to be false in part or otherwise, then without prejudice to any other action that may be taken, I/We, hereby agree to be treated as a disqualified Bidder for the ongoing Contract.

In addition to the disqualification our concern/entity may be banned/blacklisted.

AND, that I/We, shall have no right whatsoever, to claim for consideration of my/our bid at any stage and the money deposited in the form of EMD shall be liable for forfeiture in full, and the tender, if any to the extent accepted may be cancelled.

Signature of the Deponent

(Authorized signatory of the Bidder with Seal)

Date: Place:

Annexure 5: Check-list for the Technical Bid

(to be enclosed with the Technical Bid)

1. Name of the Bidder, Postal address & Registered Office:
2. Type of organization:
3. Contact name & designation of the Authorized Signatory of the Bidder & contact number:
4. Official email, phone, fax:
5. Official website:

Sl. No.	Qualification Requirement	Complied	Documents
1.	Bidder's Experience – Documents in support of meeting Technical Criteria along with **Annexure-2C** (Refer Chapter 5 and Clause 5.1)		
2.	Bidder's Experience – Documents in support of meeting Financial Criteria (Refer Chapter 5 and Clause 5.2)		
3.	Average Turn Over Certificate of Last 03 Years (Refer Chapter 5, Point – 5.2)		
4.	Incorporation related documents (Refer Chapter 5, Point – 5.3.1)		
5.	Copy of PAN & GST Registration (Refer Chapter 5, Point – 5.3.2)		
6.	Declaration by the Bidder – **Annexure-4**		
7.	Proof of payment of Tender Paper Fee (Refer Chapter 5, Point – 5.3.4)		
8.	Proof of payment of EMD/ documents related- to exemption from the same (Refer Chapter 5, Point – 5.3.4)		
9.	Self-Attested Copy of Functional office with copy of (Refer Chapter 5, Point – 5.3.6)		
10.	Self-Attested copy of Service Center details (Refer Chapter 5, Point – 5.3.7)		
11.	Copy of OEM Authorization Certificate as per **Annexure-2B** (Refer Chapter 5, Point – 5.3.8)		
12.	Quality Certificate of Bidders (Refer Chapter 5, Point – 5.3.9)		
13.	Compliance sheet on OEM Letterhead (Refer Chapter 5, Point – 5.3.10)		
14.	Copies of supporting documents from OEM related to warranty of products (Refer Chapter 5, Point – 5.3.11)		
15.	Product Certification for of UL, BIS, CE, FCC (Refer Chapter 5, Point – 5.3.12)		
16.	Copy of supporting documents showing presence of OEM in India for at least 5 years (Refer Chapter 6, Point – 6.1.3)		
17.	Copies of Site Survey (Refer Chapter 5, Point – 5.3.14)		

18.	Signed Copy of Tender Document (Each & Every page to be sealed & signed)		
19.	Signed copy of this check list with seal – **Annexure5**		
20.	Bank details – **Annexure-6**		
21.	Pre-Bid Queries – **Annexure-9**		

Date Signature of the Authorized Signatory of the Bidder with

Seal

Annexure 6: Mandate Form - on the letterhead of the Bidder

To

The Orissa State Cooperative Milk Producers' Federation
Limited (OMFED) D-2, Saheed Nagar, Bhubaneswar
Odisha – 751007

Sub: Mandate for payment through electronic mode i.e. EFT/NEFT/RTGS

Dear Sir,

We are here by giving our consent to get all our payments due from OMFED through electronic mode i.e. EFT/NEFT/RTGS. We also agree to bear all the bank charges payable in this regard.

(Please furnish the information in capital letter)

1. Name of the Bidder
2. Address of the Bidder

PIN Code			
IT PAN			
e-mail ld		Mobile No	
Phone			

3. Bank Particulars

Bank Name					
Branch Name					
Branch Address					
Account No.					
Account Type	Saving/Current/Cash Credit		Branch State		
RTGS Enable	Yes/No	NEFT Enabled	Yes/No	Core-Bank Enabled	Yes/No
Branch Code		MICR Code		IFSC Code	

4. Effective Date

We hereby declare that the particulars furnished are correct & complete. If any transaction is delayed or not effected for incomplete/incorrect information/any other technical reasons, we will not hold OMFED responsible.

Date: Signature of the Authorized Signatory of the Bidder with Seal

Certified that the Bank particulars furnished are correct as per our record.

Date: Signature of the Bank with seal

Annexure 7: Format for Performance Security

BG should be obtained from Nationalized/ Scheduled Bank and should be operable and invokable at its Branch in Bhubaneswar

(To be executed on INR 100/- non-judicial stamp paper)

B.G. No. Dated:

WHEREAS:

(A) …….. ("AGENCY") and The Orissa State Cooperative Milk Producers' Federation Limited having its office at D-2, Sahid Nagar, Bhubaneswar – 751 007 ("OMFED") has issued a Letter of Award (LoA) dated (the "LoA") whereby OMFED has agreed to engage the Agency for …… (the "agreement").

(B) The LOA requires the AGENCY to furnish Performance Security to OMFED of a sum of INR _____/- (the "Guarantee Amount") as security for due and faithful performance of its obligations, under and in accordance with the AGREEMENT, for a period of _____ (the "Guarantee Period").

(C) We,…….. through our branch at (Bhubaneswar) (the "Bank") have agreed to furnish this bank guarantee ("Bank Guarantee") as Performance Security. NOW, THEREFORE, the Bank hereby, unconditionally and irrevocably, guarantees and affirms as follows:

1. The Bank hereby, unconditionally and irrevocably, guarantees and undertakes to pay to OMFED upon occurrence of any failure or default in due and faithful performance of all or any of the AGENCY's obligations, under and in accordance with the provisions of the agreement, on its mere first written demand, and without any demur, reservation, recourse, contest or protest, and without any reference to the Agency, such sum or sums up to an aggregate sum of the Guarantee Amount as OMFED shall claim, without OMFED being required to prove or to show grounds or reasons for its demand and/ or for the sum specified therein.

2. A letter from OMFED that the AGENCY has committed default in the due and faithful performance of all or any of its obligations under and in accordance with the agreement shall be conclusive, final and binding on the Bank. The Bank further agrees that OMFED shall be the sole judge as to whether the AGENCY is in default in due and faithful performance of its obligations under the agreement and its decision that the Agency is in default shall be final, and binding on the Bank, notwithstanding any difference between OMFED and the Agency, or any dispute between them pending before any court, tribunal, arbitrator or any other judicial or quasi-judicial body or by the discharge of the Agency for any reason whatsoever.

3. In order to give effect to this Bank Guarantee, OMFED shall be entitled to act as if the Bank were the principal debtor and any change in the constitution of the Agency and/ or the Bank, whether by their absorption with any other body or corporation or otherwise, shall not in any way or manner affect the liability or obligation of the Bank under this Bank Guarantee.
4. It shall not be necessary, and the Bank hereby waives any necessity, for OMFED to proceed against the Agency before presenting to the Bank its demand under this Bank Guarantee.

5. OMFED shall have the liberty, without affecting in any manner the liability of the Bank under this Bank Guarantee, to vary at any time, the terms and conditions of the agreement or to

extend the time or period for the compliance with, fulfilment and/ or performance of all or any of the obligations of the AGENCY contained in the agreement or to postpone for anytime, and from time to time, any of the rights and powers exercisable by OMFED against the AGENCY, and either to enforce or forbear from enforcing any of the terms and conditions contained in the agreement and/ or the securities available to OMFED, and the Bank shall not be released from its liability and obligation under this Bank Guarantee by any exercise by OMFED of the liberty with reference to the matters aforesaid or by reason of time being given to the AGENCY or any other forbearance, indulgence, act or omission on the part of OMFED or of any other matter or thing whatsoever which under any law relating to sureties and guarantors would, but for this provision, have the effect of releasing the Bank from its liability and obligation under this Bank Guarantee and the Bank hereby waives all of its rights under any such law.

6. This Bank Guarantee is in addition to, and not in substitution of, any other guarantee or security now or which may hereafter be held by OMFED in respect of, or relating to, the agreement or for the fulfillment, compliance and/ or performance of all or any of the obligations of the Agency under the agreement.

7. Notwithstanding anything contained hereinbefore, the liability of the Bank under this Bank Guarantee is restricted to the Guarantee Amount and this Bank Guarantee will remain in force until the expiry of the Guarantee Period, and unless a demand or claim in writing is made by OMFED on the Bank under this Bank Guarantee no later than twelve (12) months from the date of expiry of the Guarantee Period, all rights of OMFED under this Bank Guarantee shall be forfeited and the Bank shall be relieved from its liabilities hereunder.

8. The Bank undertakes not to revoke this Bank Guarantee during its validity, except with the previous express consent of OMFED in writing, and declares and warrants that it has the power to issue this Bank Guarantee and the undersigned has full powers to do so on behalf of the Bank.

9. Any notice by way of request, demand or otherwise hereunder may be sent by hand/messenger or by post addressed to the Bank at its above referred branch, which shall be deemed to have been duly authorized to receive such notice and to effect payment thereof forthwith, and if sent by post it shall be deemed to have been given at the time when it ought to have been delivered in due course of post and in proving such notice, when given by post, it shall be sufficient to prove that the envelope containing the notice was posted and a certificate signed by an officer of OMFED that the envelope was so posted shall be conclusive.

10. This Bank Guarantee shall come into force with immediate effect and shall remain in force and effect until the expiry of the Guarantee Period (including the claim period) or until it is released earlier by OMFED pursuant to the provisions of the agreement.
11. Capitalized terms used herein, unless defined herein, shall have the meaning assigned to them in the agreement.

12. Notwithstanding anything contained herein:

i. Our liability under this Bank Guarantee shall not exceed INR .....
ii. The Bank Guarantee shall be valid up to ……. (“Expiry Date including claim period” of the Bank Guarantee).

iii. We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and if you serve upon us a written claim or demand made in the manner prescribed in this Bank Guarantee on or before …… (Claim Period of the Bank Guarantee) at our Branch at _____Bhubaneswar.

iv. After claim period all your rights under this Bank Guarantee will be forfeited and we shall be relived and discharged from all liabilities thereunder, irrespective of whether the original has been returned to us or not.

13. The Bank Guarantee is issued in paper form and Advice transmitted through SFMS with required details to the beneficiary's advising bank (INDIAN BANK, _____BRANCH, BHUBANESWAR, IFSC Code _____).

Signed and Delivered by _____Bank by the hand of Mr./Ms. _____, its _____and authorized official.

(Signature of the Authorized Signatory) (Official Seal) NOTE:

i. The Bank Guarantee should contain the name, designation and code number of the officer(s) signing the Bank Guarantee.

ii. The address, telephone number and other details of the head office of the Bank as well as of issuing branch should be mentioned on the covering letter of issuing Branch.

For _____[Indicate name of Bank]

Signature……. Full Name…….
Designation…… Power of Attorney No…….
Date……. Seal of the Bank……..

WITNESS: (SIGNATURE WITH NAME AND ADDRESS) (1)

Signature……. Full Name……..

(2)

Signature……. Full Name…….

Annexure 8: Format for Power of Attorney

(to be executed on INR 100 non judicial stamp paper and to be duly notarized)

Known all men by these presents, we ..... (name of the firm and address of the registered office) do hereby irrevocably constitute, nominate, appoint and authorize Mr./ Ms. (name), …… son/daughter/wife of …… and presently residing at ……., who is presently employed with us and holding the position of ……. , as our true and lawful attorney (hereinafter referred to as the "Attorney") to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our tender against the Bid document no. [•] dated [•] published by The Orissa State Cooperative Milk Producers' Federation Limited for the "Procurement of Services – [•]", including but not limited to signing and submission of all applications, bids and other documents and writings,

AND we hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said Attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE,……., THE ABOVE NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON
THIS
.....
DAY OF
.....
20[•].

For

……
(Signature, name, designation and address)

Witnesses

1.

2.

Accepted

(Signature)
(Name, Title and Address of the Attorney)

Annexure 9: Format for submitting Pre-Bid Queries

Bidder to submit the pre-bid queries in following format in both pdf format as well as in excel.

Sl. No.	Clause No.	Page No.	Provision of Document	Queries / Suggestions