nfai
national film archive of india
राष्ट्रीय फिल्म संग्रहालय
Where The Heritage of Indian Cinema Comes Alive ...

REQUEST FOR PROPOSAL FOR SELECTION OF MASTER SYSTEM INTEGRATOR (MSI) FOR IMPLEMENTATION OF NFAI'S ENTERPRISE SOLUTION

Tender Ref. Number: 302/52/2021 - NFHM

Date: 16 November 2021

NATIONAL FILM ARCHIVE OF INDIA
Ministry of Information & Broadcasting, Government of India
Law College Road, Pune-411004

Table of Contents

Abbreviations

Terms	Definitions
AI	Artificial Intelligence
AMC	Annual Maintenance Contract
API	Application Programming Interface
BEC	Bid Evaluation Committee
BHIM	Bharat Interface for Money
BI	Business Intelligence
BIS	Bureau of Indian Standards
BOQ	Bill of Quantity
BOT	Built Operate Transfer
CA	Certificate Authority
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CMDB	Change Management Database
CMMI	Capability Maturity Model Integration
COTS	Commercial off the shelf
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSM	Content Storage Management
CV	Curriculum Vitae
DBA	Data Base Administrator
DC	Data Center
DCP	Digital Cinema Package
DD	Demand Draft
DDoS	Distributed denial of service
DNS	Domain Name Server
DOS	Denial of Service
DPX	Digital Picture Exchange
DR	Disaster Recovery

Terms	Definitions
DRC	Disaster Recovery Centre
DRM	Digital Rights Management
DVD	Digital Video Disk
EMAIL	Electronic Mail
EMD	Earnest Money Deposit
FAQ	Frequency Asked Question
FC	Fibre Channel
FCS	Finite Capacity Scheduling
FIAF	International Federation of Film Archives
FIPS	Federal Information Processing Standard
FMS	Facility Management System
FRS	Functional Requirement Specifications
FTP	File Transfer Protocol
GB	Gigabit
GCC	Government Community Cloud
GUI	Graphical User Interface
HD	High Definition
HDD	Hard Disk Drive
HR	Human Resource
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer protocol
HTTPS	Hyper Text Transfer Protocol secure
HVAC	Heating, ventilation, and air conditioning
ID	Identification
IP	Internet Protocol
IPS	Intrusion Prevention System
ISI	Indian standard institute
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology

Terms	Definitions
ITIL	Information Technology Information Library
KDM	Key Delivery Message
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOI	Letter of Intent
LTO	Linear Tape-Open
MAF	Manufacturer Authorization Form
MAM	Media Asset Management
MeitY	Ministry of Electronics and Information Technology
MB	Mega Byte
ML	Machine Learning
MSI	Master System Integrator
NAS	Network Attached Storage
NES	NFAI Enterprise Solution
NFAI	National Film Archive of India
NFHM	National Film Heritage Mission
NIC	National Informatics Centre
OEM	Original Equipment Manufacturer
OPEX	Operational Expenditure
OS	Operating System
OTP	One-time password
OTT	Over the Top
PB	Peta Byte
PBG	Performance Bank Guarantee
PDA	Personal Digital Assistants
PDF	Portable Document Format
PM	Project Manager
QA	Quality Assurance
RAM	Random Access Memory
RDBMS	Relational database management system

Terms	Definitions
REST	Representational State Transfer
RFID	Radio-frequency identification
RFC	Request for Change
RFP	Request for Proposal
ROM	Read Only Memory
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SD	Standard Definition
SIEM	Security information and event management
SDK	Software Development Kit
SFTP	SSH File Transfer Protocol
SLA	Service Level Agreement
SLB	Server Load Balancer
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPV	Special Purpose Vehicle
SQL	Structured Query Language
SRS	Software Requirements Specifications
SSL	Secure socket layer
TB	Tera Byte
TIFF	Tagged Image File Format
UAT	User Acceptance Testing
UBA	User Behaviour Analytics
UI	User interface
UPI	Unified Payments Interface
UX	User Experience
VESDA	Very Early Smoke Detection Apparatus
VPN	Virtual Private Network

Chapter 1: Invitation of Bids

1. Disclaimer

1.1. National Film Archive of India, Pune (hereinafter referred to as NFAI or 'NFAI') has issued this Request for Proposal (hereinafter referred to as "RFP") for Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution on such terms and conditions as set out in this RFP document, including but not limited to the Technical Specifications set out in different parts of this RFP document.

1.2. This RFP has been prepared with an intention to invite prospective Applicants/ Bidders and to assist them in making their decision of whether or not to submit a proposal. It is hereby clarified that this RFP is not an agreement and the purpose of this RFP is to provide the Bidder(s) with information to assist them in the formulation of their proposals. This RFP document does not purport to contain all the information bidders may require. This RFP document may not be appropriate for all persons, and it is not possible for NFAI to consider the investment objectives, financial situation, and particular needs of each Bidder.

1.3. NFAI has taken due care in preparation of information contained herein. However, this information is not intended to be exhaustive. Interested parties are required to make their own inquiries and respondents will be required to confirm in writing that they have done so, and they do not solely rely on the information contained in this RFP in submitting their Proposal. This RFP includes statements, which reflect various assumptions and assessments arrived at by NFAI in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require.

1.4. This RFP is not an agreement by and between NFAI and the prospective bidders or any other /person. The information contained in this RFP is provided on the basis that it is non–binding on NFAI, any of its authorities or agencies, or any of their respective officers, employees, agents, or advisors. NFAI makes no representation or warranty and shall incur no liability under any law as to the accuracy, reliability or completeness of the information contained in the RFP document. Each Bidder is advised to consider the RFP document as per his understanding and capacity. The bidders are also advised to do appropriate examination, enquiry and scrutiny of all aspects mentioned in the RFP document before bidding. Bidders

are encouraged to take professional help of experts on financial, legal, technical, taxation, and any other matters / sectors appearing in the document or specified work. Bidders are also requested to go through the RFP document in detail and bring to notice of NFAI any kind of error, misprint, inaccuracies, or omission in the document. NFAI reserves the right not to proceed with the project, to alter the timetable reflected in this document, or to change the process or procedure to be applied. NFAI also reserves the right to decline to discuss the Project further with any party submitting a proposal.

1.5. No reimbursement of cost of any type will be paid to persons, entities, or consortiums submitting a Proposal. The Bidder shall bear all costs arising from, 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 NFAI or any other costs incurred in connection with or relating to its Bid.

1.6. This issue of this RFP does not imply that NFAI is bound to select and pre-qualify Bids for Bid Stage or to appoint the selected MSI, as the case may be, for the project and NFAI reserves the right to reject all or any of the Bids without assigning any reasons whatsoever.

1.7. NFAI may, in its absolute discretion but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP.

1.8. NFAI, its employees and advisors make no representation or warranty and shall have no liability (for any cost, damage, loss or expense which may arise from or is incurred or suffered on account of anything contained in this RFP or otherwise, including but not limited to the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to be part of this RFP or arising in any way with eligibility of bidder for participation in the Bidding Process) towards any Applicant or bidder or a third person, under any law, statute, rule, regulation or tort law, principles of restitution or unjust enrichment or otherwise.

1.9. NFAI also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any bidder upon the statement contained in this RFP.

1.10. Interested parties, after careful review of all the clauses of this 'Request for Proposal', are encouraged to send their suggestions in writing to NFAI. Such suggestions, after review by NFAI, may be incorporated into this 'Request for Proposal' as a corrigendum which shall be uploaded onto the e-tendering website and NFAI website: www.nfai.gov.in

2. Invitation for Bids

2.1. NFAI hereby invites Proposals for Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution. Bidders are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions, and implications.

2.2. The complete bidding document has been published on www.nfai.gov.in for the purpose of downloading.

2.3. A two stage three envelope selection procedure shall be adopted as provided in Chapter 3: Instruction to Bidders of this RFP

3. Confidentiality

This document has been circulated to invite participation from the interested Bidders who have requested for the purchase of RFP for Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution. Information shared with Bidders through this document is confidential in nature. Any further circulation of this information without prior permission of NFAI is prohibited and shall attract punishment/penalties.

4. Schedule details

S. No	Information	Details
4.1.	Tender Fee/Cost of the RFP for Selection of MSI to be paid in form of a DD from any scheduled commercial bank in name of "Sr. AO, ROB, Pune" payable at Pune	INR 10,000/-
4.2	Bid Security/ Earnest Money Deposit (EMD)	Not applicable
4.3	Publishing of RFP	November 16, 2021
4.4.	Submission of queries	November 19, 2021 up to 5 pm

4.5.	Pre-bid meeting	November 23, 2021 at 11:30 am
4.6	Site Visit to NFAI's premises	To be communicated later
4.7.	Release of response to clarifications would be available on	• *NFAI Website:* www.nfai.gov.in/ • E-Publish Website: https://eprocure.gov.in/epublish/app
4.8	Last date (deadline) for submission of bids	December 07, 2021, 3:00 PM
4.9	Opening of Technical Proposal	December 08, 2021, 4:00 PM
4.10	Presentation of qualified agencies	To be intimated later
4.11	Opening of Commercial Proposal	To be intimated later
4.12	Correspondence details	Shri. HL Guru Prasad (IIS). Officer on Special Duty, National Film Heritage Mission, Contact – (020) 29701569 Email ID - osdnfhm@gmail.com
4.13	Submission details	The Bidders should send / submit their responses to it@nfaipune.gov.in

5. Preamble

5.1. The National Film Archive of India (NFAI) was established in February 1964 as a media unit of the Ministry of Information & Broadcasting, Government of India. The mission of NFAI is to safeguard the heritage of Indian Cinema for posterity and act as a Center for dissemination of healthy film culture in the country. NFAI has a large collection of filmic and non-filmic material belonging to every period and era of Indian cinema.

5.2. NFAI has a vast collection of film reels, photos, posters, song booklets, pamphlets, press clippings, and books. The detailed account is provided in the subsequent sections.

5.3. NFAI encourages and promotes research and academic activities related to various aspect of Cinema. It assigns monographs about eminent Indian filmmakers and pioneering film personalities, research fellowships on themes pertaining to Indian cinema, and audio-visual history recordings of senior artists and technicians. As part of its activities related to disseminating film culture, NFAI has a Distribution Library which supplies films to various film societies, educational institutions, and cultural organizations in the country. It also conducts special screening programs across the country and is a major source of films for international film festivals in India and abroad.

5.4. The Ministry of Information & Broadcasting, Government of India has launched the National Film Heritage Mission with an objective of Preservation, Conservation, Digitization and Restoration of filmic heritage of the country. Nearly 5000+ Feature Films and Short Films are proposed to be digitized and restored under this Mission.

5.5. Both digitized/ restored films and born digital films, together with digitized non-filmic content shall be an input to the NFAI's Enterprise Solution (NES) for web based digital access to media assets (filmic and non-filmic).

6. Objective of the RFP

The purpose of this RFP is to seek the services of Master System Integrator (MSI), who shall Design, Build, Maintain, Operate On-Cloud Data Center, On-Cloud Disaster Recovery Center, and an On-Premises Media Ingestion Room. The MSI shall also Design, Customize, Procure, Supply, and integrate a software solution (NFAI Enterprise Solution & NFAI Website) including its Deployment, Commissioning, Licensing, Hosting and Maintenance. The scope shall also include Change Management, Amendments, Operations and Services of the complete solution for implementation of NFAI's On-Cloud Data Center along with Enterprise Solutions (NES) and website under National Film Heritage Mission (NFHM) at NFAI for a period of 5 years post Go-Live

This document provides information to enable the bidders to understand the broad requirements to submit their bids, however the bidders should conduct their due diligence to broaden their understanding. The detailed scope of work is provided in Chapter 2: Scope of work of this RFP document. NFAI reserves the right to amend the scope of work.

Chapter 2: Scope of Work

1. Scope of work

Background

1.1. NFAI has a large collection of assets related to films, deposited/acquired through various sources. These assets include Film Reels, Posters, Books, Pamphlets, magazines etc. As a part of NFHM project, landmark films are undergoing digitization and restoration while non-filmic assets are being digitized.

These digitized assets will be stored in LTO Tapes. The process for digitization and restoration of the selected films and their hosting on an enterprise solution is illustrated as below:

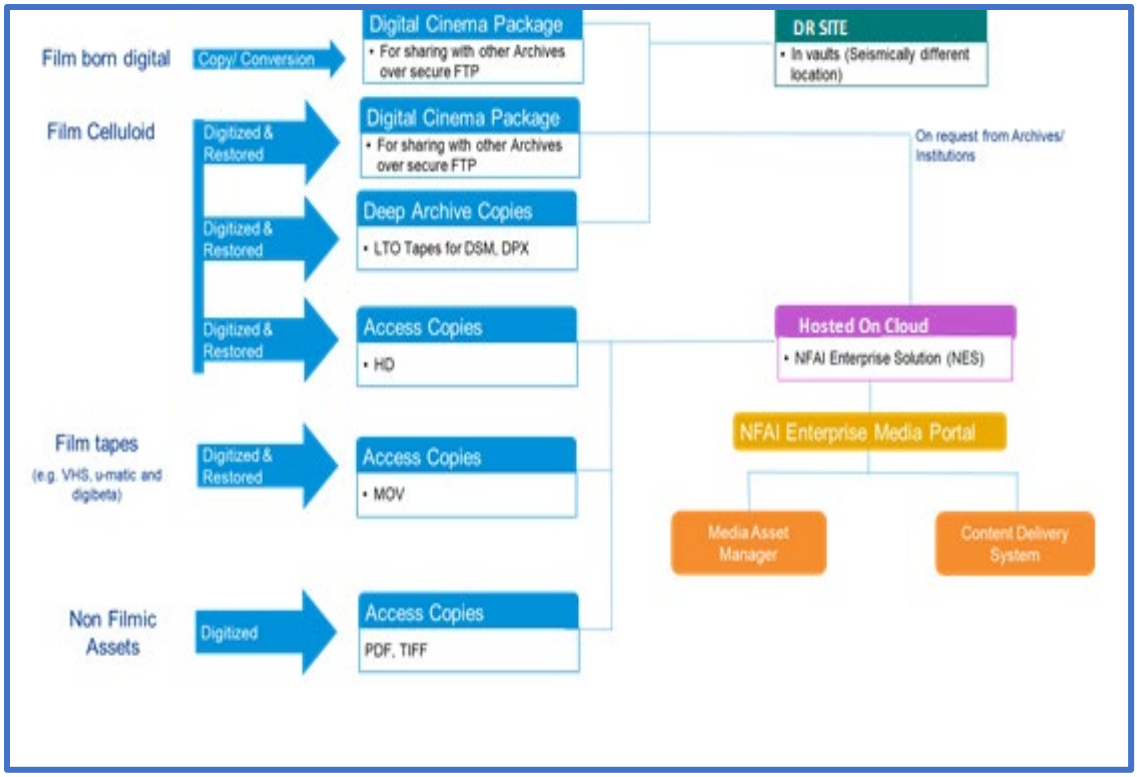

Figure 1 Digitization and restoration of the selected films and their hosting on an enterprise solution

1.2. The MSI will be required to manage different file formats post their output from digitization and restoration stage and maintain their copies on LTO tapes, as follows:

#	Particulars	Format	Metric	Storage Media	Quantum (per format)
1	Filmic material	DCP HD	No. of films	LTO7 or higher version tapes	5,113
2	Born Digital Films	DCP HD	No. of films	LTO7 or higher version tapes	1,200
3	VHS	MOV	No. of films	LTO7 or higher version tapes	1,500
4	U-matic Tapes	MOV	No. of films	LTO7 or higher version tapes	3,000
5	Betacam & Digibeta	MOV	No. of films	LTO7 or higher version tapes	5,500
6	Non-filmic material	PDF, jpeg	No. of pages	LTO7 or higher version tapes	475,722

Note: The numbers above are indicative and subject to change.

1.3. Filmic data distribution

#	Particulars	Format	Metric	Storage Media	Quantum (per format)	File size
1	Filmic material	DCP HD- Feature (F) HD – Short (S)	No. of films	LTO7 or higher version tapes	5,113	0.25 TB F - 0.09 TB S – 0.02 TB
2	Born Digital Films	DCP HD	No. of films	LTO7 or higher version tapes	1,200	0.25 TB 0.09 TB
3	VHS	MOV	No. of films	LTO7 or higher version tapes	1,500	0.002 TB
4	U-matic Tapes	MOV	No. of films	LTO7 or higher version tapes	3,000	0.002 TB

#	Particulars	Format	Metric	Storage Media	Quantum (per format)	File size
5	Betacam & Digibeta	MOV	No. of films	LTO7 or higher version tapes	5,500	0.002 TB
6	Non-filmic material	PDF, jpeg	No. of pages	LTO7 or higher version tapes	483,920	Provided in Table Below

1.4. Non – Filmic data distribution Volume

#	Particulars	Quantity (Nos)	Size of each file(in MB)	
			JPEG	TIFF
1	Wallposters	38,182	20 - 30	90 - 100
2	Song Booklets	22,228	5 - 9	3 – 7
3	Pamphlets	5602	2 - 7	2 - 5
4	Stills	208,288	10 - 30	10 - 12
5	Slides	10,260	5 - 20	5 - 7
6	Press Clippings	199,360	5 - 12	5 - 9
7	**Total**	**483,920**		
8	**Total Size estimate (in TB)**		**1**	**8**

Note: The numbers mentioned above are indicative and are for providing a broad overview of the quantum at NFAI

1. Inputs to the solution

Only HD access copies of selected titles, approved by NFAI shall be hosted on the proposed NFAI Enterprise Solution (NES) which will reside in cloud along with Non-Filmic Data.

The ingestion of Filmic and Non-Filmic Data into the NES shall be done from the Media Ingestion room which will be built in NFAI premises which will also house the Automatic Tape Library with the Robotic Arm. The Disaster Recovery site shall operate at 100 % replica of the Primary Data on Cloud.

Below are various types of data that shall reside on the cloud.

#	Project/ Activity list	Cloud	Disaster Recovery
1	Digitization and Restoration – Features and Short Films	HD (On-demand)	HD On-demand)
2	Previously Restored	HD (On-demand)	HD (On-demand)
3	Non-filmic material	Access Copy (.pdf)	Access Copy (.pdf)

2. NFAI Enterprise Solution – Hosted on Cloud

2.1. The NFAI Enterprise Solution shall be hosted on MeitY emplaned Virtual Private Cloud and shall provide adequate space to store all the Filmic as well as Non – Filmic assets of various programs envisioned by NFAI. The NES shall meet the need for reliability, availability, scalability, security, and interoperability.

2.2. On Cloud Disaster Recovery

2.2.1. Disaster Recovery shall be a 100% replica of the NFAI's Enterprise Solution.
Disaster Recovery should be hosted on MeitY empaneled cloud. In case of a disaster when the on-cloud data center's services get affected, it shall be the responsibility of the MSI to ensure uninterrupted services to the user, meeting all the SLA requirements defined in the RFP.

2.3. Media Ingestion Room

2.3.1. The Media Ingestion room shall be housed in NFAI Premises

2.3.2. The Media Ingestion room shall host the Media Ingestion Server

2.3.3. The Media Ingestion Room shall host nodes (computers) attached to the Media ingestion server

2.3.4. The server in the Media Ingestion room shall be connected with Automatic Tape Library

2.3.5. The Source content will arrive at NFAI premises from the digitization and restoration vendor only in LTO Tapes as part of the scanning and digitization output. As part of the Media Ingestion Room responsibilities, the MSI:

(a) Shall perform compatibility check for uploading to cloud any digital content received from external source, other than the Digitization & Restoration

vendor . The compatibility parameters will be finalized after consultation with NFAI. The Compatible File Format shall be in line with MP4 HD.

(b) Shall rectify the problems as far as possible

(c) Shall transcode the source file to the required NFAI file formats for uploading on to the NES cloud portal.

(d) Shall provide the equipment and resources to carry out the ingest services at NFAI premises.

2.4. Project Go Live

The proposed NFAI Enterprise Solution will be hosted on MeitY empaneled Virtual Private Cloud. The Go Live shall be achieved within 6 months from the date of signing of the contract.

2.5. Digitization and Restoration Project

2.5.1. This project includes scanning and digitizing approximately 5,113 titles (including feature and short films). LTO-7 (or higher) will be the medium of storage and the digitized output shall be made available in various formats such as DPX, DCP, Apple ProRes, HD, and SD (H.264).

2.5.2. Of the 5,113 titles, approximately 2,253 titles shall undergo restoration process which shall be done by multiple vendors. The output from Restoration project shall be similar to the Digitization project output in form of LTO-7 (or higher) as the storage medium.

2.5.3. Outputs from Digitization and Restoration projects in the medium of LTO7 shall be made available on a periodic basis to the MSI in format required to be uploaded to the cloud through the Ingestion room. The output in the LTO 7 tapes is of type DPX, WAV, Mov, .MP4, .MKV, DCP.

2.6. Accession of Born Digital Films

NFAI is in a constant process of receiving born digital films and it is envisaged to make copies of these films available on the NES platform via on-demand basis. The MSI is expected to add these titles (in digital format) post transcoding in the required format in the asset management catalogue along with a promo of the same.

2.7. Non-Filmic material

NFAI is in custody of several non-filmic assets such as Posters, Books, Pamphlets, magazines etc. Most of these assets have undergone digitization and the scanned copy in true resolution and compressed resolution format have been stored at NFAI server. The MSI shall provide access to NFAI users (such as researchers and film scholars, etc. as defined in the user access (Chapter 2: Section 15.1) through NFAI's web portal and through a mobile application.

All users by default shall be given HD resolution copies to be viewed and downloaded of the Non-Filmic material. High Resolution copies shall be made available to selected registered users through the User request portal of the NES portal, post approval from NFAI while displaying access copies for rest of the registered users.

2.8. Digitization of Magnetic Tapes

NFAI also has films in magnetic tapes such as U-matic, Betacam, Digibeta and VHS and shall undergo restoration (if required) and digitization. These digitized formats shall be provided to the MSI for incorporating into the asset management and the MSI shall make the content available on the Enterprise Media Portal along with a promo if required by NFAI

3. Solution Scenario

The MSI is required to Design, build, operate, and maintain the NFAI enterprise solution on a MeitY empaneled Virtual Private Cloud along with Disaster Recovery which would enable enterprise grade, one-stop, web window comprising of NFAI Enterprise solution for its all the users to access.

The scope further covers the requirements study, solution design, solution development, testing, implementation, hosting of scalable and agile NFAI Enterprise Solution and Maintenance for 5 (five) years post Go-live of the solution.

4. Overview

The broad services that the MSI needs to provide includes (but not limited to):

1.1. Data Center hosted on Cloud

1.1.1. The expected minimum scope of work is detailed under this section. The MSI shall add additional components as they feel are required to meet the requirement given in the

Service Level Agreement. The MSI has to provide the complete solution and fill all the gaps which are not covered in this RFP.

The proposed scope of work for the MSI has been broadly divided into seven categories.

1. System Integration Services

Design, Procure, implement, and commission all the IT (active and passive) components required to deliver a complete solution

2. System Maintenance Services

Undertake maintenance services of all the components being procured and installed through this RFP to ensure that overall uptime commitment as defined in SLA section (Service Level Agreement) of the RFP

3. OS and Database support services

Provide administration, patch upgrade and update management services for OS and Database for the solution

4. Performance Monitoring and Capacity Management Services

Procure, operate, and maintain the monitoring components and provide performance monitoring and capacity management services for the solution

5. Messaging Services

Provide Unified Messaging Services to the authorized users of NFAI.

6. Application Related Services

Provide certain Application related services like Application Maintenance / Enhancement / Migration.

7. Operation and Maintenance of NFAI Web portal

Provide services related to operations and maintenance of NFAI web portal www.nfai.gov.in

1.1.2. Proposed Cloud Architecture must have a storage capacity of 100 TB of data and the storage shall be upward scalable based on the growth and demand in the next five years. In addition to this a deep archival storage on cloud shall be provisioned having a storage capacity of ~500TB of data. (Refer Chapter 6: Section 4.3)

1.2. Disaster Recovery Center on Cloud

1.2.1. Disaster Recovery Center shall be hosted on MeitY empaneled cloud

1.2.2. Disaster Recovery center shall be a 100% replica of DC (hosted on cloud).

1.2.3. It shall be responsibility of the MSI to ensure uninterrupted operation of NFAI Enterprise solution at all times.

1.3. Tape Library and Maintenance

1.3.1. MSI to deploy, operate and maintain Tape Library with three (3) drives and One (1) Robotic Arm with minimum 500 slots (The robotic arm should be able to support 500 slots on day one). Of the three drives in the Tape Library Two Drives Shall be LTO 7 and One Drive shall be LTO 9. The Tape Library should be expandable, and the robotic arm should be able to support up to 1500 slots in the future. The required scalability should be with the addition of modules or frames. The robotic arm must be able to support cater to all the number of slots after expansion.

1.3.2. The LTO tape library will house only the LTO tapes which have Access copies and shall be the responsibility of the MSI.

1.3.3. To develop, operate and maintain LTO drive interface to transfer content from LTO to local storage as per requirement.

1.3.4. MSI shall be responsible for storing and management of LTO tapes in a secure environment in the NFAI premises

1.3.5. DELETED

1.3.6. MSI shall be required to procure Approx. 13,000 LTO 7 tapes. As per the current estimate, the required number of LTO7 tapes for the NES project is approx..11,000. **Any quantity purchased by NFAI over and above the 11,000 LTOs the MSI shall be paid on actuals.** For content acquired by NFAI during the project period above and beyond the quantum specified in the RFP, MSI shall be responsible for copying of content on storage medium (LTO7 tape or higher). The storage medium will be procured by MSI.

1.3.7. For the aforementioned number of LTO Tapes, the MSI shall be responsible for procuring and handing over the tapes to NFAI. However, the MSI shall be responsible for configuring the LTO Tapes to the MAM solution.

1.3.8. The LTO Tapes which has raw data (DPX and WAV files) shall be stored in **Phase 3 of NFAI premises in the digital vault.** The management, operation & maintenance of the digital vault shall be the responsibility of NFAI.

1.4. Local Central Storage

1.4.1. MSI to shall deploy, operate, and maintain the Local central storage in the Media Ingestion Room

1.4.2. The Local Central Storage will primarily be utilized for post-production activities and intermediate storage before ingestion of content to cloud

1.4.3. The Local Central storage shall have a minimum of 30 TB Raw capacity using SSD drives and 500TB Raw capacity using SAS 10K Drives Storage

1.5. NFAI Enterprise Solution

1.5.1. To develop, operate and maintain the on-Cloud data center as per the requirement mentioned in below sections

1.5.2. To develop, operate and maintain the facility for continuous data transfer (ingestion) of digitized and restored filmic and non-filmic material from LTO tapes and Local central storage to the Enterprise solution on cloud.

1.5.3. To develop, operate and maintain Media Asset Management (MAM) system for physical and digital media assets.

1.5.4. To develop, operate and maintain an enterprise portal that will allow multiple Users (Chapter 2: Section 15.1) to access the available content in accordance with access rights defined by NFAI.

1.5.5. To create published and unpublished archival finding aids according to archival standards on the portal.
Definition of Finding aids: Finding aids are tools that help a user find information in a specific record group, collection, or series of archival materials. Examples of finding aids include published and unpublished inventories, container and folder lists, card catalogs, calendars, indexes, registers, and institutional guides.

1.5.6. To develop, operate and maintain an OTT platform with payment gateway to access filmic and non-filmic content as per predefined user privileges defined under Chapter 2: Section 15.1.

1.5.7. To develop, operate and maintain CMS (Content Management System) for uploaded and stored data

1.5.8. To develop, operate and maintain filmic and non-filmic on Demand system for transfer of content requested by users to develop, operate and maintain a streamlined DCP on Demand system for transfer of content to requesting agencies such as film festivals/ archives.

1.5.9. To integrate the entire solution as per proposed architecture

1.5.10. Integration of multiple content catalogues and development of a master catalogue to be used/ made available to NFAI

1.5.11. To develop, operate and maintain a mobile application for entire NFAI Enterprise solution.

1.5.12. All the rights of the developed solution shall be with NFAI. MSI needs to handover the complete solution including Physical Infrastructure, whenever required and suggested by NFAI after completion of the contract.

1.5.13. The developed Enterprise solution shall be capable of ingesting and processing datatypes, beyond the discovered datatypes of NFAI (mentioned in the RFP). The NES shall be capable of metadata tagging of these datatypes.

1.5.14. The solution designed shall be based on scalable, agile platform with a service- orientated architecture.

1.5.15. The workflow designer shall be such that it lets the NFAI administrator create and modify workflows in-house with no scripting knowledge needed.

1.5.16. NFAI Enterprise solution shall have an intuitive web-based search mechanism and restore user interface

1.5.17. MSI shall provide manual and automated workflows for archives and restores.

1.5.18. MSI shall incorporate integrated proxy viewer that shall aide in user to browse, select clips and perform partial restore for remote files.

1.5.19. NES shall provide reporting on archived content usage

1.5.20. NES shall have functionality of capturing comprehensive audit trail of all archives and restores.

1.5.21. MSI shall provide a portal for NFAI administrator to enable configuration options basis user groups defined in the RFP.

1.5.22. NES should have a content queue management in place to ensure timely delivery of requested content.

1.5.23. The system should be able to perform tape integrity verification and checksum activities.

1.5.24. The NES shall have a simple watch folder/XML ticket interface or full RESTful API.

1.5.25. For quantum of material acquired by NFAI during the project period, which is above and beyond the numbers indicated in the RFP, MSI shall be responsible for copying, transfer, transcoding, metadata tagging and cataloguing of the content. MSI shall be responsible for copying the content on the storage medium of LTO 7 or higher as approved by NFAI.

1.5.26. The list of functionalities indicated above are minimum essential requirements from NFAI and are not an exhaustive list.

1.6. Media Ingestion Room

1.6.1. To develop, operate and maintain the facility for continuous data transfer (Ingestion) of digitized and restored filmic material and digitized non-filmic material from LTO to NES hosted on cloud.

1.6.2. MSI to build a Media Ingestion room to facilitate the Tape Library, Local Central Storage, ingest server, transcode servers, editing and QC workstations along with the required network and network security for secured connectivity

1.6.3. MSI to ensure secure data transfer from Media Ingestion Room to NES hosted on Cloud

1.6.4. MSI to ensure that the data transfer to cloud to happens securely & seamlessly

1.6.5. MSI to ensure that the data is encrypted at Rest and while in motion

1.6.6. MSI to supply Tape Library with Robotic Arm as part of the Media Ingestion Room solution

1.6.7. MSI to ensure at least 2 workstations are provided in the Media Ingestion Room for editing and at least 2 workstations are provided for content QC

1.6.8. MSI to ensure that local central storage is utilized of storing postproduction data

1.6.9. MSI to facilitate one-time bulk transfer of data from Media Ingestion Room to Cloud

1.6.10. MSI to provide dedicated P2P link from Media Ingestion Room in NFAI to On Cloud Data Center

1.6.11. MSI to provide dedicated bandwidth (1:1) to Media Ingestion Room

1.6.12. Within the Media Ingestion Room, MSI shall ensure commissioning of necessary hardware and software setup for performing read/write operations over Blu-Ray, DVD and Hard Disks.

1.6.13. MSI to commission requisite hardware and software for Post-Production activities that will happen from the Media Ingestion Room. The following lists a broad list of activities that the MSI shall be responsible for in the said component:

1.6.13.1. Perform Editing of film clips for the social media request and researchers
1.6.13.2. Exporting films/ titles for catering to requests from film festival and researchers
1.6.13.3. Creation of encrypted DCPs with KDM for film festivals
1.6.13.4. Color Grading of digital films, as and when required by NFAI.
1.6.13.5. Export content from the digital contents from LTOs, DVDs, Blu-Rays, and other storage media
1.6.13.6. To process Born Digital material
1.6.13.7. Picture and Audio QC of digital material received by NFA
1.6.13.8. Editing photographs, song booklets etc. for any special request

5. System Integration Services

The MSI should undertake a complete infrastructure life cycle management for providing required services for the NES solution This would include:

- Analyze
- Design
- Procure
- Implement

5.1. Analyze

MSI should analyze the project requirements, its present status, the applications hosting plan, the existing infrastructure, and any other relevant details before designing the On Cloud data center and quoting prices.

5.1.1. Study of current storage requirement

The MSI shall study the service requirements of present storage required in NFAI as well as estimate requirement of the any other storage that are in the conception stages.

5.2. Design

The MSI will be free to design the architecture and / or specifications given as part of this RFP on the basis of initial study that they would carry out as part of the "analyze" scope of work given

above, subject to the approval by NFAI. Any component level up gradation if required shall be allowed with NFAI approval. However, any cost revision shall not be allowed due change in design.

5.2.1. Design validation and change

The MSI shall prepare detailed deployment design document (both Application & Hosting) and shall submit the same for approval within 30 days of the signing of the contract.

The MSI shall also prepare detailed application deployment document for NFAI and shall submit the same for approval along with the migration support document for this application.

While preparing the design the MSI shall keep in mind the scalability requirements as mentioned in the RFP

5.3. Procure

The MSI shall procure the materials and equipment as required and given as part of the MSI's response. However, it should be noted that the MSI is expected to procure all necessary equipment's to run the Media Ingestion Room n case, it is identified that certain components are required but not quoted by the MSI, The MSI will procure the same free of cost for NFAI. The MSI shall note that the specification provided is the minimum requirement and the MSI shall procure better equipment if it is required to meet the service levels mentioned in Service Level Agreement(SLA)

The MSI shall procure and supply all components and subcomponents (Active as well as passive), as per requirements of the RFP/Contract. The specification of the equipment's is mentioned in RFP. All the software's used for providing postproduction services shall be licensed to NFAI and will be the property of NFAI.

The MSI shall be responsible for end-to-end implementation and shall quote and provide/supply any items not included in the bill of material but required for commissioning of the NFAI's Enterprise Solution. NFAI shall not pay for any such items, which have not been quoted by the MSI in the bid but are required for successful completion of the project.

The MSI shall supply all the installation material/ accessories/ consumables (e.g., screws, clamps, fasteners, ties anchor, supports, grounding strips, wires etc.) necessary for the installation of the systems.

The MSI has to prepare and submit a delivery report including details of all components supplied. The delivery report will be validated by the identified NFAI person.

Any additional equipment procured by MSI, will be supplied by their respective OEM.

The MSI would be responsible for inventory check, testing and installation of the equipment accordingly and coordinating with the supplier as required.

5.4. Implement

MSI shall provide a complete On Cloud data center with 100% disaster recovery solution along with the Media Ingestion Room to NFAI as a part of their technical bid. Any activity not mentioned here but required for the implementation, operation, and maintenance and monitoring of the On-Cloud data center with 100% disaster recovery and the Media Ingestion Room shall be implemented. The solution provided by the MSI shall meet all the service level requirements.

5.4.1. Equipment installation and configuration

MSI will be expected to bring all the installation equipment's and tools required for the installation of the system. The MSI shall install and commission the Media Ingestion Room along with active network equipment as well as passive network components (Cabling etc.) as per approved deployment design. The backbone network infrastructure shall be minimum 10 Gbps. All the work shall be done in a conscientious manner as per the OEM guidelines and best industry practices. The system shall be subjected to inspection at various stages. Local regulation / codes shall be followed at all times. The MSI shall follow all Safety Regulations and practices.

The MSI shall not cause any damage to Government buildings /other premises and property and will perform restoration if any damage occurs. The MSI shall plug conduits and entrance holes where the cabling has been installed with suitable sealing material.

The MSI shall configure all the components and sub-components for end-to-end user access to applications/services.

The MSI shall be responsible for the installation and configuration of software applications/modules for the Enterprise Management and security management, etc.

5.4.2. Connectivity

The MSI shall be responsible for setting up dedicated P2P link between the NFAI Media Ingestion room and the Cloud Setup.

MSI shall be responsible for providing non-shared internet bandwidth to Media Ingestion Room. Seamless integration with independent Internet Service Providers shall be provisioned by the MSI.

5.4.3. Acceptance Testing

The acceptance test for the Enterprise Solution shall be carried out by NFAI or duly appointed third party agency by NFAI. The MSI should cooperate with the third-party agency to ensure successful completion of Acceptance tests.

NFAI or any Third-Party Agency appointed by it shall undertake the acceptance testing and will also be responsible for verification; validation of all the invoices submitted and will recommend eligible payments according to milestones.

The acceptance test shall consist of a Final acceptance test (FAT). The MSI shall submit a detailed acceptance testing document and NFAI and the MSI shall mutually agree upon the same.

i. Final acceptance Test:

After successful installation of in accordance with the requirements in the RFP, Final Acceptance Test shall be conducted where in-service level parameters will be tested for at least 30 days of trouble-free operation. After the successful testing of NFAI Enterprise solution On Cloud Data Center test environment, shall be put to live usage in the NFAI's On Cloud Data Center. After successful commissioning of the application in NFAI cloud Data Center, all the concerned service parameters will be tested for at least 15 days.

Final Acceptance Certificate shall be issued by NFAI to the MSI after successful testing of this application.

The date on which final acceptance certificate is issued shall be deemed date of the successful commissioning of the On-Cloud Data Center. Any delay by the MSI in the performance of its contracted obligations shall render the MSI liable to the imposition of appropriate liquidated damages, unless agreed otherwise by tenderer.

5.4.4. Training and Documentation

After installation has been completed, the MSI shall provide training to a batch of NFAI staff for 3 (Three) months at the NFAI Media Ingestion Room. This training shall be held before Go-Live of

the application. MSI shall provide a second training two years after Go-Live of the solution for a period of another 3 (Three) months. All the required training material will be provided to the participants by MSI. The training shall cover all aspects of the solution, not limited to the Media Ingestion Room equipment, software, Data ingestion, cloud, and disaster recovery maintenance and generating reports an involved in the buildup of on NFAIs Enterprise solution and shall be provided by Certified Professionals.

The MSI shall document all the installation and commissioning procedures and provide the same to NFAI within one month of the commissioning of Enterprise Solution and the Media Ingestion Room.

The MSI shall submit a complete cabling system layout (As installed), including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways for the Media Ingestion Room at NFAI.

Manufacturer's technical documentation on all devices used in the system including user manuals for configuring of and their 'As installed' configuration shall be provided by the MSI.

The MSI will also provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation.

Process documentation: The MSI shall be responsible for preparing process documentation relating to operation and maintenance of each and every service as mentioned in this section. The prepared process document shall be formally signed off by NFAI before completion of final acceptance test.

The process documentation shall include but not limited to the categories of scope defined above. Each process map shall clearly define the roles and responsibilities, detailed steps for execution the defined task, detailed configuration steps etc.

6. Operation & Maintenance Services

Under the scope of Operation & Maintenance Services MSI shall undertake monitoring, administration, management, and maintenance of the Official Web site of NFAI along with Media Ingestion Room infrastructure supplied, installed, and commissioned by the MSI.

The MSI shall ensure that all the devices that will be installed in the Media Ingestion Room as part of the physical infrastructure should be SNMP enabled and shall be centrally monitored and managed on a 24x7 basis.

The MSI will monitor the performance of the on-cloud data center components including usage, availability and analyze the future requirements if any. In case the requirement exceeds the scalability, requirements mentioned, the MSI has to upgrade the current cloud infrastructure in order to meet the increase in demand.

The MSI should undertake proactive monitoring of the entire deployed infrastructure and diagnose problems that could arise as part of any component installed at the Media Ingestion Room. The MSI should maintain a log of all such diagnosis and notify the NFAI on a monthly basis in the form of a report

All faults that have been identified would need to be isolated and rectified appropriately. The report mentioned above would include resolution measures undertaken by the MSI and results produced accordingly.

Proactive and reactive maintenance, repair, and replacement of defective components (IT and Non-IT/ Hardware and Software) installed at the Media Ingestion Room through this RFP. The cost for repair and replacement shall be borne by the MSI.

Adequate onsite and offsite spare parts and spare component must be maintained by the MSI to ensure that the uptime commitment as per Service Level Agreement (SLA) is met. To provide this service it is important for the MSI to have back-to-back arrangement with the OEMs. The MSI would be required to provide a copy of the service level agreement signed with the respective OEMs.

Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the MSI fails to meet the above standards of maintenance, there will be a penalty as specified in the Service Level Agreement (SLA).

The MSI shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by NFAI at any time.

Although NFAI shall provide the security for the building, Physical Security of the Media Ingestion Room Infrastructure will be the responsibility of the MSI.

The MSI shall provide software updates for the components supported by them in the On-Cloud data center and the Media Ingestion Room for a period of five years from Go-Live. This will include the patch upgrade or any type of upgrade for, management software, operating systems, network management software, security software, anti-virus software or any other software. Software updates will be part of the supplies, at no additional costs.

7. Storage Services

The MSI shall provide this service to NFAI and shall be responsible for installation and configuration of the storage system in the Media Ingestion Room and management of storage environment to maintain performance at desired optimum levels

The MSI shall be responsible for development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.

The MSI shall configure SAN whenever a new application is hosted . This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.

8. Security Services for Ingestion Room

Security is one of the most important aspects of the Media Ingestion Room. The detailed scope of services for security are given below in order to ensure complete security of the Media Ingestion Room.
In general, the MSI shall ensure the following:

- Integration of all security components used in the Media Ingestion Room
- Secured network access provision for all authorized users
- Configure network management policies for managing all the network and security devices using network management systems
- Malicious code (virus, worms, spyware, adware) infected desktops/servers should be isolated so as to prevent further spreading.
- Secure access to centralized applications
- Formulate and Implement access rules for Media Ingestion Room to be connected to On Cloud Data Center and for VPN access to NFAI network. This would include appropriate Anti-Virus rules and general security policies.
- Adherence to all security guidelines issued by NFAI from time to time.

- The MSI would need to engineer a secure and resilient infrastructure to manage user access to information assets. The MSI would also need to understand the underlying security objectives and determine process control objectives; categorize all resources used to facilitate a process (applications, website URL, etc.) and create the ability to centrally manage all system users.
- Engineering security and controls within hardware and software components would also have to be looked at by the MSI. In this respect, the MSI would need to select and implement one or more means to verify a user's identity; implement a mechanism to apply access controls to computing resources; establish permissions for resources; configure non-user-based security options.
- The MSI would need to engineer controls to ensure network processes are performed in a reliable and repeatable manner. A collection of control activities which satisfies the network objectives and provides control over a process should be put in place. The MSI should also typically create a logical grouping of entitlements and link users with developed roles according to the job function.
- The MSI would need to develop and implement processes and technologies that provide secure access to resources. In this respect, the MSI should deploy the hardware and software components which enable a network process or provide security. The MSI should also develop and implement the appropriate training needed to deploy security initiatives and inform users of new policies.

A completely secure on cloud data center is of utmost importance to NFAI. All the security strategies and methods developed by the MSI as according to guidelines given earlier, would need to be operational and implemented. Continuously managing the security and controls built across the infrastructure of processes and technologies would be one primary facet of the Operational aspect of the security cycle. This activity includes updating, enhancing, and monitoring the technology environment.

The MSI's responsibility would be to continuously manage a secure environment, monitor for anomalous events, implement appropriate mitigating controls, integrate with the core IT environment, and escalate appropriately if events become incidents or emergencies. The MSI shall be responsible for 24/7 security monitoring of the on-cloud data center.

The MSI needs to resolve security issues by maintaining an up-to-date environment, including patching vulnerable systems, and applying incremental additions and security configuration updates to existing systems.

Any security incident would need to be met by an appropriate security response by the MSI's team. A timely response would be essential in order to minimize loss. It would be the MSI's responsibility to put in place an appropriate response mechanism to take care of any security incidents. The MSI would need to adopt any practice necessary to reduce the impact of the incident, assess damage, and ensure that the network quickly recovers from the attack and provides all on cloud data center services. In this respect, major areas which the MSI would need to look at include:

- The MSI would need to ensure minimal damage by deploying an Incident Response Team (Helpdesk), which will attempt to limit the number of systems affected and the amount of processing that is interrupted.
- Resolve, through technical or policy means, the inherent vulnerability from which the incident stemmed, thus preventing its recurrence.
- Determine what happened, how the incident occurred, what systems were affected and what information was compromised, gathering evidence to pursue legal action if appropriate.
- Ensure operational functionality is restored by reestablishing systems – applying patches, adding software/hardware, and conducting other remediation as required.

In addition to the general methodology discussed above, Media Ingestion Room shall have in place a Firewall system, an Intrusion Prevention System, and an Anti-Virus Solution.

The proposed equipment should include the required Hardware and Software solutions. The minimum required technical standard of these equipment are mentioned in the RFP

The MSI shall carry out the following activities with respect to this equipment:

- Installation & configuration of firewall & IPS
- Defining security policy for firewall & periodic review of the firewall configuration.
- Log generation, Analysis & Report for Firewall system & IDS/IPS
- Incident management structure for firewall & IDS/IPS shall be defined by MSI.
- Reports for firewall & IDS/IPS shall be submitted by MSI on monthly basis. The MSI shall, in due consultation with NFAI, finalize format for the reports & its frequency.
- Configure the Anti-Virus Solution according to requirements and ensure that the solution is up to date with the latest patches and upgrades.

9. OS, Database, Applications and Licenses support services

- The MSI shall be responsible for end-to-end management of database, Application, and licenses on an ongoing basis to ensure smooth functioning of the same.
- The MSI shall undertake management of changes to database schema, disk space, storage, user roles.
- Conduct code and configuration reviews to provide tuning inputs to NFAI in order to improve the application performance or resolve bottlenecks if any.
- Undertake performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database and applications as required.
- The MSI shall provide management of database upgrade or patch upgrade as and when required with minimal downtime as per the Service Level Agreement (SLA).

- The MSI shall take regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.
- The MSI shall provision and use of DBA tools related to performing database creation, maintenance, and database monitoring tasks

10. Performance Monitoring and Capacity Management Services

Capacity Management ensures that the performance of services, capability of handling, storing, and managing the required volumes of information by the infrastructure meets the On Cloud Data Center requirements.

Another aspect of the Capacity Management responsibility is to identify appropriate new technology and propose its adoption where this will be cost-beneficial to the organization.

The MSI shall ensure that 3 major areas for Capacity Management are regularly monitored, assessed, and managed. These 3 areas include:

10.1. Business Capacity Management

As regards the Business Capacity Management the MSI shall need to have mechanism in place to access the future service requirements based on input from their future plans and Service Level Management requirements. This includes growth and expansion plans as well as new services required for these, or to better support current activity. Data on existing services and their usage and performance patters will also form an important input.

10.2. Service Capacity Management

For Service capacity management the MSI shall monitor, measure, and analyze the performance of the IT services, their use of resources, working patterns, etc. The responsibility here shall ensure that the services can and do meet their Service Level Agreement (SLA) targets.

10.3. Resource Capacity Management

The MSI as a part of resource capacity management shall focus on the actual components, their performance and its utilization like current infrastructure technology, resilience of systems and services, Future, or alternative technology

The MSI shall undertake following sub- activities to enable them to perform the 3 major activities mentioned above. The sub-activities include:

- The MSI shall perform continuous monitoring to ensure that resources and services perform as required to meet the terms of the Service Level Agreement (SLAs). Monitoring would include items regarding capacity (e.g., throughput) and performance (e.g., response time). Monitoring is performed on the basis of thresholds set by technical specifications and Service Level Management. For performing this activity, the MSI would be required to deploy an EMS which would continuously monitor the links, network devices, servers and provide statistics about the components in the On Cloud Data Center such as Disk Space (logical/Physical), memory usage, swap, paging, CPU idle (for all in case of multiple CPU system), http, interface traffic, etc.
- The MSI would be required to analyze the data with a view to identify trends of utilization and service level so that a normal or baseline can be determined.
- There after the MSI shall undertake regular monitoring and comparison with this baseline and identify exception conditions or near misses in the Service Level Agreement (SLAs). Analysis can be used to predict future resource usage, or to monitor actual growth against predicted growth.
- The MSI shall perform tuning which identifies measures to improve either utilization or performance levels for a specific device or service. The changes are then proposed via Change Management procedure articulated separately

  The MSI shall make available these reports on a periodic basis to the NFAI

11. Operations & Maintenance

Following are the summary of operations and maintenance services to be provided by the MSI to be performed under the supervision of NFAI. It shall include but not limited to:

11.1. Media Ingestion Room

- MSI shall provide comprehensive onsite support on official working hours of the weekdays and holidays if required by NFAI basis to ensure an uptime of 99.95% for the NES application hosted on cloud, the cloud infrastructure, and the IT infrastructure solution at the Media Ingestion Room in accordance with the Service Level Agreement mentioned as part of this tender.
- MSI shall commit to provide all necessary manpower resources onsite to resolve any issues/incidents and carry out required changes, optimizations, and modification.
- MSI shall assign onsite manpower resources on official working hours of the weekdays (i.e., 9:30am to 6.30 pm) and holidays if required by NFAI to diagnose, troubleshoot, and resolve issues related to the Media Ingestion Room services and Enterprise solution. The onsite

support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc. MSI shall also provision for necessary offsite support to ensure continuity of operations for NES.

- MSI shall provide comprehensive technical support services for all the hardware and software proposed for the entire period of the contract. The technical support should include all the upgrades, updates and patches that are released by the respective OEMs during the period of contract.
- MSI shall provide comprehensive onsite warranty on 24 x 7 x 365 basis for a period of 5 (Five) years from the date of Go-Live of all IT infrastructure provided as part of scope of this tender. The warranty period shall commence from the date of acceptance of the entire system only.

11.2. Cloud Hosting

The MSI shall be responsible for providing 24*7*365 days support for NFAI Enterprise Solution on Cloud infrastructure for 5 years from Go-Live. It shall include but not limited to:

- Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000:1, for maintaining operations of cloud and ensuring privacy of NFAI data
- Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP
- In the event of a disaster at cloud DC site, activation of services from the cloud DR site is the responsibility of MSI. The MSI shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate cloud DR site. Cloud DR drills needs to be performed by the MSI half yearly to check disaster preparedness.
- The MSI shall conduct vulnerability and penetration test at their cost (from a third-party testing agency which should be CERT-IN empaneled and approved by NFAI) on the Cloud facility every 6 months and reports should be shared with NFAI. The MSI needs to update the system in response to any adverse findings in the report, without any additional cost to NFAI
- Upgrades - Any required version/Software / patch management etc. on the Cloud will be supported by the MSI for the entire contract period at no extra cost to NFAI
- MSI is required to provision additional VMs when the utilization exceeds 90%

11.3. NFAI Website

The MSI shall maintain and Support the Website for a period of 5 years after the successful Go-Live of NFAI website. It shall include but not limited to:

- Upgrades, which would include version releases made by the MSI to incorporate technological changes, consolidating all bug fixes, consolidating all enhancement requests made by NFAI

- Modifications would include minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of NFAI website. Any UI / UX change shall be considered as part of the maintenance activity. However, in case the application goes under a service layer / business layer change, then the same may be considered as part of the Change Request.
- Enhancements would include changes in the software due to Statutory and Regulatory changes and changes required due to changes in industry and other Governance practices in India.
- Any changes required on the design / placement of the elements or the contents on the home page or any internal page/s of the website.
- Any change request would be mutually agreed between the MSI and NFAI as per the change request clause.
- Maintenance and up keeping of any upgrades of the solution.
- Providing all software updates and patches released by the OEM (if applicable), update and patch management, resolution of any issues / problems with the solution etc.
- Resolution of errors / bugs (if any), software updates, changes in the software that may be necessary due to legal/statutory changes etc.
- Troubleshooting of any incidents, issues, bugs, errors etc. reported with regards to any application and rectification of same within time of issue logged as per timelines of SLA.
- Provide handholding support and training services as part of the post implementation services, on a scheduled basis as well as on a need basis.
- Perform system administration tasks such as managing the user access, creating, and managing users, preparing MIS reports etc.
- Performance tuning of the NFAI websites to ensure adherence to SLAs and performance requirements as indicated in the RFP.
- User support in case of technical difficulties in use of the software solution, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental.
- Prompt receipt, analysis and reporting of reported deficiencies in the operation of the website solution and supply of information and advice on such deficiencies.
- Unscheduled, on call, corrective and remedial maintenance, and support services.
- Integration of existing and envisaged 3rd party, software modules, API's, web-views as per the requirement of NFAI
- At the end of term of 5 years, NFAI may continue services and extend the term of the contract depending upon the performance of the Agency. However, in case NFAI wishes to engage a new Agency for support / maintenance or any other enhancements, MSI shall be responsible for handover to new Agency appointed by NFAI within a period of 2 months with all necessary documentation, source code, etc.

11.4. Minimum Qualification & Experience of key personals required during O&M period

S.N.	Roles	Role Responsibility	Qualification & Experience (Indicative)
1	Project Manager	• Creating and Maintaining Project Plans and Organizing work environment • Manage Project Risk and Client Expectations • Promote Communications and Coordination at all organization level • Help Ensure milestones are met and quality is delivered • Ensure documentation of Project Activities	• Full-Time Graduation Degree in Engineering • Post-Graduation degree or above in Business Administration or Computer Science/ Computer Applications or equivalent • PMP/PRINCE2 Practitioner Certification • Minimum 10 Years of Work Experience • Experience of managing turnkey project including software solution, IT hardware implementation and Cloud hosting
2	Postproduction Expert	• Experience in deploying such hosted media asset management technology and digital archiving • Must have prior experience in handling jobs in broadcast engineering -tape based • Coordinate the electronic transference of magnetic media	• Any Gradate / Post Graduate Degree/ Diploma holder • Minimum of 7 Years' Experience in Postproduction Operation /Media Ingestion Room management
3	Network Expert	• Network Fault Monitoring & Performance Management with parodic Reporting • Network Configuration Automation • Network Traffic Flow Analysis System	• B.E. / B. Tech/MCA or equivalent with 5 Years' experience including minimum 2-year experience in Data Center / Cloud/ Postproduction Center / Ingestion Room Operation management with OEM Certification like CCNA/JNCA or equivalent
4	Tape Library Expert	• Store and maintain LTO tapes to provide Tape Library users access to relevant content necessary. • Organizing Media Section • Classify and Re-Shelving • Taking Backups • Facilitating in accessing, searching, browsing, navigating, indexing, Storing, organizing and dissemination of Digitized information	• Any Degree/ Diploma or certificate course equivalent • Minimum of 5 Years' • Experience in Tape Library Maintenance and management along with trouble shooting Skill. Relevant industry / OEM Certifications

S.N.	Roles	Role Responsibility	Qualification & Experience (Indicative)
5	Cataloguing Expert (Librarian/ Archivist)	• Classify the resources. • Catalogue the resources. • Put the data into the databases with proper keywords.	• Any Degree in Library and Information Science / Library science / Museology / Archival Science • Minimum of 5 Years work Experience with a minimum one-year experience in a film library or in a film archive or in a media library or in a media archive or in a museum • Knowledge of cataloguing and classification of books and non-book materials such as CDs, DVDs, Celluloid Films, VHS Cassettes, Posters, Photographs, Film Slides and Web resources.
6	Website Developer	• Collaborate with development team to define and implement innovative solutions for, visuals and experience • Execute all visual design stages from concept to final hand-off to engineering • Conceptualize original ideas that bring simplicity and user friendliness to complex design roadblocks • Create wireframes, storyboards, user flows, process flows and site maps to effectively communicate interaction and design ideas	• Any Degree/ Diploma or certificate course in graphic designing, Video Editing • Minimum of 3 Years' Experience in Designing Graphical User Interface of Website Portal

12. Change Management services

The MSI shall implement and manage change management procedures with following objectives:

- To manage the process whereby changes are requested, assessed, authorized, monitored, and implemented
- To ensure that no unauthorized changes are implemented
- To minimize disruption caused by changes, during and after implementation
- To ensure that changes are properly researched, options proposed and that all relevant parties have input into the assessment of changes
- To coordinate the effort involved in building, testing, and implementing changes, dealing with any slipping or excess against the agreed change and plan.

The MSI shall ensure

- That the Change Management System is properly created and implemented
- Identification of staff involved in specific roles, training and obtaining buy-in Ongoing Basis
- Unauthorized change is identified, and appropriate action taken
- Review and evaluation of existing processes to improve on turnaround for the business while managing the costs and risk to acceptable levels
- Record keeping of changes
- Review of changes to improve the process and activities involved in Change

The MSI shall ensure that for any change within the On Cloud data center to take place, a change request will undergo the following stages:

12.1. Change Initiation

A change requestor should be able to initiate a change request formally. Some changes are to meet changes in legal requirements and cannot be rejected without the Change Control Board as formulated by NFAI approval. User requested changes may be filtered through their line management. This streamlines the process, removing impracticable, conflicting, or duplicate requests.

12.2. Initial Filtering and logging

Changes not already logged by the requestor should be formally logged into the system. Each Request for change shall have a unique number.

The Change Manager (or designated alternate in change administration) filters out impractical, duplicate, or undesirable requests. If these are rejected at this stage the requestor should have a process for appeal.

12.3. Initial Priority

This is where Urgent Change requests are distinguished from Normal Change requests. There should be clear rules or guidelines as to what are the reasons a change could be called urgent.

12.4. Change Categorization

At this stage, change sought through the change requests is categorized. This is determined by several factors including:

- The possible impact of the change – positive and negative
- The cost of the change and of its impact on long term management. This includes resources required in the build, test, implementation and long-term use and management phases
- The time it will take to build, test, and implement

ITIL standards identify 3 basic categories of changes:

- Category 1: Minor impact and few additional resources required
- Category 2: Moderate impact or moderate resources required

- Category 3: Major impact or major resources required

To achieve categorization there may be a requirement for a solution or solutions to be proposed and evaluated for cost, resources and time required which the MSI shall evaluate and convey in due consultation with NFAI.

12.5. Assessment Approval and Authorization

The MSI shall follow the 3 basic levels of assessment, approval, and authorization for a change request:

- **Level 1** – Change manager (or senior change administration staff) have the authority to approve and schedule. If there are any doubts, they should forward the change to the NFAI Media Ingestion Room team.
- **Level 2** - The RFC (Request for Change) needs evaluation and discussion by the NFAI team, either electronically, or if consensus cannot be reached, then in the meeting.
- **Level 3** – The decision on this size/complexity/risk/cost has to be made at NFAI Technical Committee level.

12.6. Scheduling

Assigning resources and checking for over-allocation of resources, this in essence plots the critical path for all IT related activity that can be planned. Understanding peak or critical processing periods, change freeze periods etc. allow better scheduling.

12.7. Building the Change

The team/person assigned will put the change together. Purchasing, set-up etc. are all part of building the change. This is the first stage during which the time, cost and functionality targets can be assessed, and slippage notified to the change manager who can take the appropriate action.

Testing, implementation, and the back-out plans are all to be completed within this stage. Testing plans should be reviewed by someone other than the builders.

12.8. Testing the Change

This should be done by independent testers. The issue is frequently that the builders see what they thought they were creating and may miss vital evidence of problems, or not perform full negative testing. Where possible the requestor should be able to evaluate if the tested change delivers what was expected.

12.9. Pre-Implementation change

This stage includes confirmation of test results, back-out plan, implementation plan and resources. Any other checks that must be made before going live E.g. Training for users, support and Service Desk staff is complete.

12.10. Implementation

The implementation is coordinated by the Change Management team, who is the decision maker on when to implement the back out plan should the implementation take too long or have failed.

12.11. Monitor and Review

During and after implementation of a change, monitoring of the effects is done to assess the success of implementation. During this time any incidents or problems arising from the change must be linked to the change record to assist in the evaluation.

Many smaller similar changes may be reviewed together. Major changes or those causing major disruption should be reviewed individually. This is to improve the learning process, both to reinforce success as well as learn from failure. New changes arising from this change may be identified and logged.

12.12. Final Documentation

A change management database (CMDB) should be created and updated at various stages, depending on the nature of the change. At this stage, confirmation that all documentation has been correctly completed is necessary before closing the change.

This includes, Change Management system, CMDB through Configuration Management, user and technical documentation, operational guides for operational staff, help desk scripts etc.

14. Messaging services

The MSI shall provide messaging services to all the authorized users specified by NFAI. The MSI shall be responsible for designing, implementing and maintenance of the entire messaging solution on cloud as part of the NES

The MSI shall build and deploy centralized messaging solution including necessary software as required. It shall be the responsibility of these for complete migration from existing system to new centralized messaging system including messaging clients.

The messaging software shall adhere to the following parameters:

1. The messaging software OEM should be a leader in independent market research reports like Gartner, Radicati, IDC etc.
2. The messaging software should be open source.
3. The messaging software should provide a native offline desktop client for windows/mac
4. The messaging software should have open API to integrate business applications using MASHUPs

The MSI shall be responsible for

- Maintaining the messaging application
- Adding / removing / renewing Mail IDs on NFAI's request.
- Troubleshooting any problems in the messaging system and messaging client.
- Monitoring the mailbox usage.
- Ensuring timely dispatch of mails.
- Keeping a track on the mails getting dropped and taking backups of the mailboxes at regular intervals.

- Monitoring the performance statistics including mail server utilization statistics, memory management, CPU utilization and disk space utilization according to the Service level agreement.
- Maintaining and troubleshooting spam/content filter applications
- Regular update of Blacklist / whitelist and manual spam filter rules.
- Implement appropriate content filtering / mining mechanism,
- Prepare log report from Messaging system including Anti-Spam & Content Filtering for reporting the incidents of SPAM mails, Virus Mails & Accessing the restricted sites/contents. The report to be submitted to the designated NFAI office on periodic basis for review and taking corrective actions with consultation of the Project management consultant.
- Implement and maintain gateway level SMTP antivirus and Antispam.
- All incoming and outgoing mail traffic shall be routed through gateway antivirus and checked/ verified to be malicious content free.

15. Proposed architecture

The MSI Shall be responsible for the procurement, installation, testing, Solution development/ customization, deployment and maintenance as mentioned in the scope of work. All the facilities/ services shall be developed, deployed, and maintained by the MSI for NFAI. The MSI is expected to design and deploy the Enterprise solution on MeitY empaneled Cloud along with 100% Disaster Recovery in Cloud along with setting up of Media Ingestion Room within **6 months from date of signing of contract.**

The high-level architecture of the NFAI Enterprise Solution is as follows:

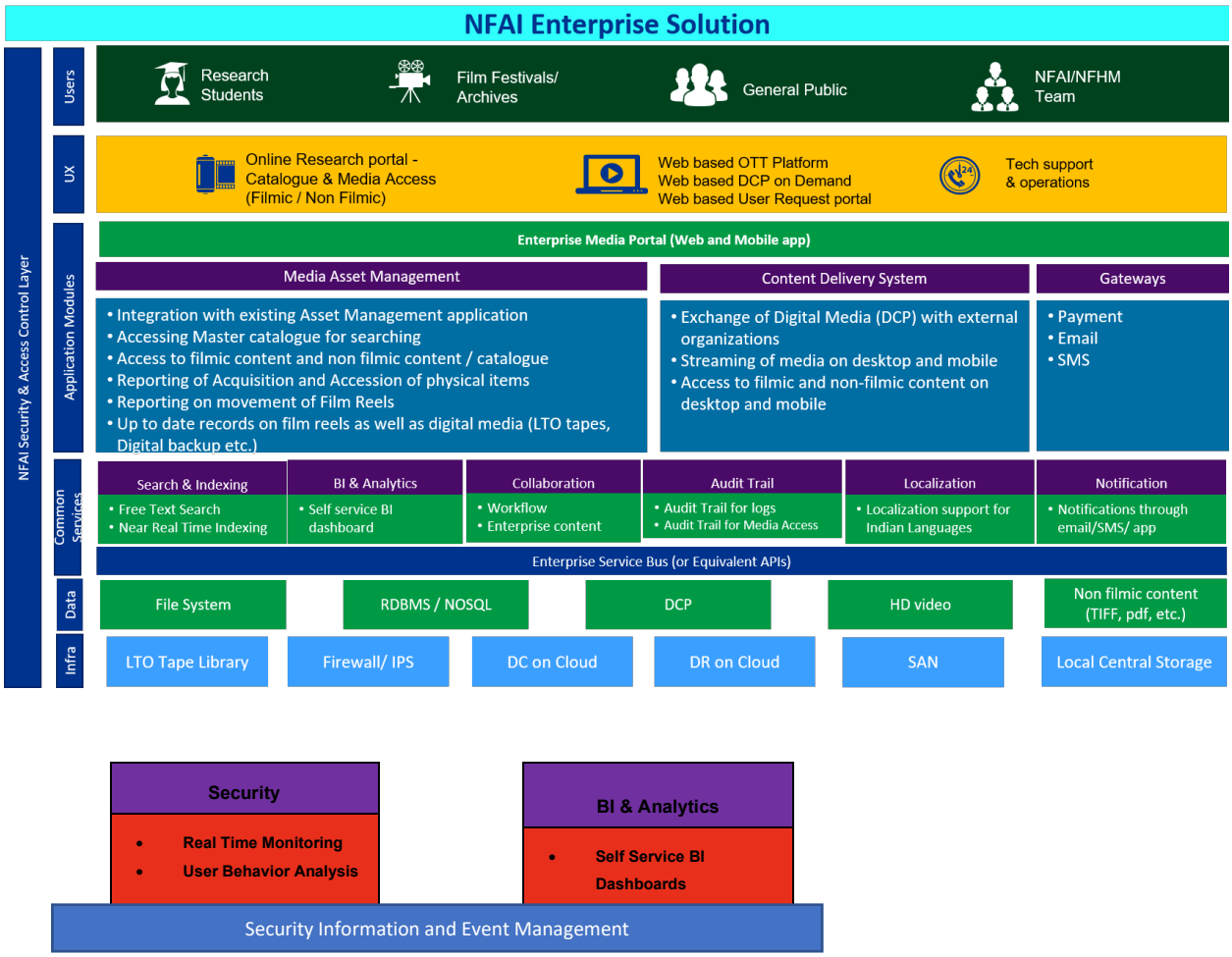

Figure 2 High Level Architecture of the NFAI Enterprise Solution

The following sections further describe the requirements under each layer:

15.1. Users

The uppermost layer represents the users of the Enterprise Web Portal Solution.

The users of the Enterprise Web Portal Solution shall be as follows:

15.1.1. General Public: Will have access to Standard streaming in high definition (HD) versions of films over the internet (whenever the content is made available).

15.1.2. Research Scholars: Will have restricted streaming/ downloading functionality, basis the privileges defined under Chapter 2: Section 15.1 Table, for easy offline access on the mobile device with NES application only

15.1.3. Film Festivals/ Archives: Will have access to DCP formats of requested films

15.1.4. NFAI/ NFHM Team: who would like to browse through information related to Catalogue & contents as well as reports and dashboards related to all the modules.

Users will get access to the portal and underlying functionalities depending on their user profile and privilege levels. Access to the system will be defined as follows:

Privilege Level	User Profile	Access
1	General Public	OTT Platform Access
2	Research Scholars	OTT Platform Access Filmic & Non-Filmic Content catalogue Access
3	Film Festivals/ Archives	On Demand DCP Transfers
4	NFAI/ NFHM Team (~15 users)	Key Personnel will get open access to Catalogue, Media Asset Management, Dashboards and all the modules

15.2. User Interface

This layer provides access to users of the services provided by the Enterprise Solution. Following are the services provided by the UX layer:

15.2.1. Catalogue & Media Access

15.2.2. Streaming and DCP on Demand

15.2.3. Users Request Module

15.2.4. Tech support and Monitoring Assets

15.2.5. Other Applications if any

15.3. Application Modules

The UX layer will be served by underlying applications which has all the functional modules as mentioned in this NFAI Enterprise Solution (NES).

15.3.1. Enterprise Media Portal

At the very minimum, the MSI will be required to develop and maintain an enterprise portal that will act as a single interface access to the entire gamut of services for users

based on privilege access levels. The following are indicative specifications for the portal:

15.3.1.1. Should have an interface for login and new user registration.

15.3.1.2. Should capture all relevant information during user registration, thereby, enabling mapping of the new user to the user group defined under Chapter 2: Section 15.1

15.3.1.3. Relevant information as cited above, will be finalized after due consultation with NFAI.

15.3.1.4. Proposed portal will be single integrated user interface for all stakeholders. Backend bespoke applications will be exposed through Portal console using single sign on.

15.3.1.5. Portal should enable personalization and configuration at user level.

15.3.1.6. The portal should be capable of directing relevant content and information to individual users/ roles, basis the user privileges defined under Chapter 2: Section 15.1, and thereby provide an end user customization.

15.3.1.7. Portal should enable content publishing within portal framework. It should support or should be capable of integrating with an advanced content management solution.

15.3.1.8. The portal should not allow concurrent sessions for same user. The system should automatically log out a customer in case of session breakdowns (e.g., communication failure, high inactivity period)

15.3.1.9. The portal should implement security features, such as configurable password complexity, configurable automatic blocking (temporary/permanent) of user logins after 3 unsuccessful login attempts, password recovery options, controlled access to content stored on the portal and logging of security incidents. It should by its own or through an integrated Identity Management solution be capable of managing security rights and privileges by individual, group, and role, and should support Single Sign On.

15.3.1.10. Portal should support HTTPS protocol on Secure Socket Layer (SSL).

15.3.1.11. The portal should support the leading web browsers and must not be limited to Google Chrome, Internet Explorer, Firefox, Microsoft Edge, etc. including standard backward compatibility.

15.3.1.12. The portal should provide search engine with advanced full-text search capabilities. The search engine should be able to search for requests within the portal.

15.3.1.13. Should provide support for comprehensive audit trail features as mentioned in section Chapter 2: Section 15.4 of this RFP.

15.3.1.14. Portal should be interoperable with industry standard databases (Oracle/ DB2/ Microsoft etc.)

15.3.1.15. Portal should be capable of supporting multilingual content capabilities

15.3.1.16. Portal should be compatible and operable on mobile devices (both Android and iOS)

15.3.1.17. Should integrate with email servers and instant messaging services

15.3.1.18. Should integrate with any other portal products through open standards such as HTML, XML, web services, etc.

15.3.1.19. Be accessible from NFAI's home page (www.nfai.gov.in) either through a widget or dedicated link or dedicated Icon on the main page with user login for authentication, similarly for External users and through an intranet for NFHM personnel accessing the system on NFAI premises.

15.3.1.20. Enable users to browse the catalogue of filmic and non-filmic assets preserved by NFAI

15.3.1.21. Enable NFAI to monitor, control & manage access & utilization of its huge, digitized media assets

15.3.1.22. Enable NFAI to monitor, control & manage access & utilization of its physical media assets stored in vaults & library. An RFID based asset tracking mechanism is already in place at NFAI storage vaults. MSI shall integrate the existing asset tracking software onto its media portal.

15.3.1.23. Enable streamlined process for transcoding which will enable the users to work on the files seamlessly irrespective of file formats (DPX/H.264 etc.) and storage media (LTO tapes/ Disks/ etc.)

15.3.1.24. All the functional modules will reside under the portal. This system will be hosted on MeitY empaneled Cloud.

15.3.1.25. Additionally, above functionalities & features are indicative in nature. The proposed solution by the MSI must encompass all the necessary and relevant features to make it scalable in nature. This must be updated & finalized in consultation with NFAI only.

15.3.1.26. System should have facility to manage and provide Multi linguistic preferences.

15.3.1.27. System should allow user to manage their preferences of available data.

15.3.1.28. System should allow user to make payment on requirement through all online modes e.g., UPI, BHIM, Net banking, Mobile banking, Card payments etc.

15.3.1.29. System should be able to retrieve the details of available registered payment applications under the selection of the payment mode option.

15.3.2. Media Asset Management (MAM) System

The MAM system will contain information about all the assets (Physical or Digital) related to all the works that are in possession of NFAI. The MAM system manages all videos, images, graphics, and documents, and lets users easily find, use, organize, manage, and share digital assets in a Web UI. The proposed MAM system should have following functionalities:

i. Should provide a search window interface with advanced search options. The window should seamlessly search across the data inventory across different catalogues and provide search results in a user-friendly interface.

ii. Should be able to seamlessly synchronize with the existing application prepared as part of Film Collection Assessment for keeping the Metadata up to date. Existing cataloguing standard is EN 15907 complaint. The MSI should be able to manage all NFAI collection data as per archival industry standards. Whether cataloguing, managing locations and movements or archive conditions, deployed solutions should adhere to archival cataloguing standards.

iii. Should be compliant with OAIS Reference Model

iv. Should be able to integrate databases provided by multiple vendors during digitization, restoration of filmic assets and during digitization of non-filmic assets and create a master database for the same

-In master database, MSI should be able to manage data at work, manifestation, variant, and item levels and ensure the appropriate links between related works.

- Filmic material catalogue shall be made available through APIs. Catalogue from the preceding stages (such as Film Collection Assessment, Preventive Conservation, Digitization Restoration projects) shall be made available by NFAI to the MSI on Excel. However, MSI has to collate and create a master catalogue for the NFAI Enterprise Solution.

Note: The cataloguing software should adhere strictly to standards and practices stated in 'The FIAF moving image cataloguing manual'.

v. Should support managing and documenting information and tasks related to assets entering NFAI, including acquisition or loan records, receipts, record of the reason for the deposit of the asset, and record of the asset's return to its owner.

vi. Should be able to integrate with the already functioning RFID solution designed for real time asset tracking of reels (Physical assets) in vaults

vii. Should be able to centrally upload content with permission level access

viii. Should provide automated AI tagging of video content with learning capabilities

ix. Should provide search pattern analysis

x. Should be able to manage data / logs of the temporary transfer of responsibility of an asset from other Film Archives or Film Festivals or vice versa, including loan agreements, loan history, records of costs and payments, packing lists, and records of overdue loans.

xi. Should be able to manage and document assets being de-accessioned and leaving NFAI's collection, either by transfer, sale, exchange, or destruction/loss, including transfer of title, records of approval, and reason for disposal.

xii. Should provide flexible metadata structure to add/update/delete nodes to create structure for multiple categories.

xiii. Should be able to configure ingestion of digitized films and non-filmic digitized assets in the file formats specified in Chapter 2: Section 1 to On Cloud data center.

xiv. The application should have the ability to accommodate Cataloguing guidelines to be implemented as per 'The FIAF moving image cataloguing manual': https://www.fiafnet.org/images/tinyUpload/E-Resources/Commission-And-PIP-Resources/CDC-resources/20160920%20Fiaf%20Manual-WEB.pdf

xv. Sorting and filtering based on tags and/or parameters should be available

xvi. Should be able to work as a standalone application. However, should be seamlessly integrated with Portals, Web Sites, mobile App using open standard frameworks.

xvii. Should be seamlessly integrated with all other modules mentioned in this RFP.

xviii. Should have user-based access to the catalogue at different level of privileges.

xix. Should provide restricted streaming/ downloading functionality, basis the privileges defined under Chapter 2: Section 15.1, for easy offline access on the mobile device with NES application only.

xx. The MAM application should have a workflow mechanism to link all the associated files for same Metadata Tag asset (HD, SD, MP4, metadata, subtitle track, DPX, WAV etc.) into a single instance . Furthermore, this instance essence should also have a mechanism to link the barcode of LTO tape(s) that will hold the DPX version files in an offline mode. This

linkage should be provided in the form of a barcode(s) captured using a barcode scanner and stored as a metadata field for that instance.

xxi. NFAI has adopted the Cinematographic Works Standard EN 15907 ("CWS") for its moving image cataloging and for its non-video (posters, photographs, and other ancillary material) collection. MAM and Cataloging software should be "EN 15907 Standard compliant"
The MSI needs to follow MARC 21 cataloguing standards for the cataloguing of non-video materials like books, articles, and magazines.

xxii. The software should adhere to archiving standards like EN15907 and be OAIS compliant.

15.3.3. Content Delivery System

The MSI is required to build functionalities to enable dissemination of digital media for consumption by users.

15.3.4. DCP on Demand

i. Should provide a catalogue of films with relevant information like bit depth, resolution, synopsis, file format, size, user reviews, film name (as per International standards) etc. to Film Festivals/ Archives/ Institutions. Relevant information as cited above, would be finalized after due consultation of MSI with NFAI.

ii. Should be able to process a DCP request by any authorized film festival/ archive/ institutions

iii. Should be able to verify copyright status before proceeding with user request

iv. Should be able to manage delivery of DCPs and Key Delivery Message (KDMs) to film festival/ archive/ institutions over the web. NFAI currently has DaVinci Resolve 14 for DCP generation and DaVinci Resolve or EasyDCP KDM generator for KDM generation.

v. Should be able to ensure the DCPs are accessed by only digital projectors of authorized film festival/ archive/ institutions

vi. Should ensure DCPs are always encrypted with time specific KDMs, when being delivered to film festival/ archive/ institutions over the On-Cloud data center setup.

vii. Should enable selection of timeslots of DCPs only for stipulated timelines as agreed between the requesting institution and NFAI

viii. Automation of the entire process of processing DCP requests as much as possible, with bare minimum manual intervention on behalf of NFAI staff

ix. Should provide free text search functionality for DCP files. In addition, automated metadata search and predictive search should also be included.

x. Sample DCP architecture is shown below. The MSI can suggest alternative options based on the architecture they deem appropriate.

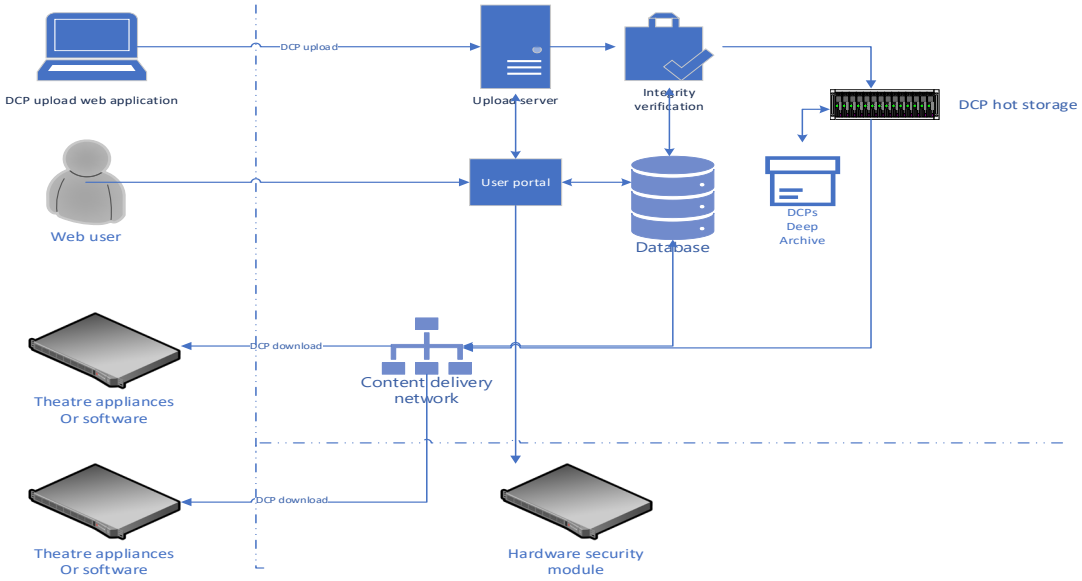

Figure 3: Sample DCP Architecture

15.3.5. OTT Platform

The proposed OTT platform should enable viewers to select restored and digitized NFAI film titles, and stream seamlessly on the device of users' preference. The following features are required on the OTT platform:

i. The OTT platform should be available through a microsite on the Enterprise Media Portal.

ii. The platform should enable users to access HD files of filmic content and should also support datatypes of non-filmic content.

iii. The access to anyone of the above-mentioned formats shall be dependent on the bandwidth availability at user's interface and the application/ software should be able to auto re-negotiate the bit rate for an optimal user experience.

iv. Should provide multi factor authentication through use of OTP type mechanism.

v. Should allow users to register on the platform with a mandatory OTP verification via SMS/ phone/ email

vi. Should provide free text search functionality for HD files. In addition, automated metadata search and predictive search should also be included.

vii. Search output should display the name of the film along with several metadata tags assigned to the film including language, year of release, sub-titles etc. or any other attributes as specified by NFAI

viii. The platform should have restricted access to only registered users with pre-defined privilege rights specified under Chapter 2: Section 15.1.

ix. A registered user should be able to make a request for a particular film among the titles available on the OTT

x. The HD copy of the required content will be retrieved by the on-cloud server and will be processed via encoding

xi. Advanced video encoding techniques will be applied on the HD copy of the requested content, which should be dependent on following factors:

   a. Efficient use of available bandwidth
   b. Playback Device of the user i.e., compatibility with a range of devices such as laptop, tablet, smartphones etc.
   c. Available bandwidth speed of the user (range of internet speeds in India on both mobile networks and broadband services) should be considered

xii. Quality (Resolution) requested by user

   i. 1080p (Bit rate ≈ 8Mbps*)
   ii. 720p (Bit rate ≈5Mbps*)
   iii. 480p (Bit rate ≈2.5Mbps*)
   iv. Auto, Adaptive Bit Rate (ABR) should be used to assess the optimal quality for streaming

   *Please note recommended bit rate numbers are indicative

xiii. Video encoding should result in visually lossless compression

xiv. The content (processed video after encoding) before being delivered should have security features to prevent illegal copying by means of any software or web-based apps

xv. The final content streamed by the registered user should have a hidden digital NFAI watermark (forensic watermark), which should map to the details of the registered user accessing the specific content, thus enabling an audit trail

xvi. Should provide functionality of offline content viewing within the application post receiving adequate permission from NFAI basis the defined user privileges under Chapter 2: Section 15.1.

xvii. The OTT platform should be able to handle at least 100 concurrent users from Go-Live with, option of upward scalability on number of concurrent users to 500. MSI to consider organic growth in the number of concurrent users

xviii. User interface (UI) of OTT should let viewers navigate the selection of films in the smoothest manner possible, and should be visually appealing

xix. UI should have sections and sub-sections for the selections of films, to facilitate NFAI the option of curation for specific titles

xx. Users should be able to search available films on the basis of Release Year, Director, Cast or any other attributes as specified by NFAI

xxi. Should be able to provide on-the-fly DRM encryption facility for secure delivery of content across the OTT platform

xxii. System should allow user to manage their preferences of available data

xxiii. System should have facility to manage and provide linguistic preferences

xxiv. The entire O&M of the OTT platform is to be managed by the MSI for the contract period. Apart from regular O&M, various other requirements from time to time would need to be incorporate during the contract period.

xxv. MSI may suggest their own architecture for developing the OTT platform.

xxvi. Should be able to provide option of switching on/ off for subtitles. Subtitles shall be provided by NFAI for select movies.

15.3.6. Gateways

The system should integrate with SMS Gateway, Email Gateway, Payment gateway etc. This would be required during user registration and user authentication based on OTP. MSI will be required to provide services of SMS, Email and Payment Gateway for all the users of NES.

15.4. Common Enterprise Services

These services are used by all the application modules. Following are critical common service functionalities:

15.4.1. Search & Indexing: for providing free text search facility across all the applications. Near real time indexing for the Catalogue and actual content will make the search more efficient and accurate.

i. Enterprise search platforms should have the capacity of searching and to support all types of structured, unstructured, semi-structured, social media, web content, enterprise systems etc.

ii. Should support search and contextualize results based on user profiles and roles.

iii. Should be able to search information from all possible data sources present in the ecosystem

iv. The search solution should support automatic query suggestions.

v. The solution should index data and documents from a variety of sources such as: file systems, system databases and other integrated external systems.

vi. Should have futuristic capabilities like context-based search, machine learning and natural language processing capabilities, content analytics and searching with subjective questions or phrases etc.

vii. The search platform must be scalable to search all the records.

viii. The search engine should have the ability to securely search internal, external systems or applications preferably without needing to index them at all times.

ix. The search should show results to the user based on the authorization and authentication of the user.

x. Security profiles of the underlying systems should be respected so that users can only see the information for which they are authorized.

xi. The search platform should be easy to customize. A web-based intuitive administrative interface is preferred.

xii. Search users should be able identify and extract specific entities relevant to their interest area fairly easily and quickly.

xiii. The search platform should support dynamic categorization of results in order to accelerate searching process.

xiv. The search platform may automatically identify and cluster related information to achieve better user satisfaction.

xv. The system must be able to search, filter and publish results (available in various formats) and on multiple parameters like demographics, education levels, interest areas etc.

xvi. The proposed system must have a search feature which should be capable of including full word matches, partially matching words, misspelt words.

xvii. The proposed system should have capability of crawling different structured and un- structured data sources

xviii. The proposed system should have a feature for specifying stop words that should not be included in the search i.e., "and", "for", "with", "from", etc. should not be considered for deciding the search results

15.4.2. BI & Analytics: This functionality will generate user-based reports and provide information in a graphical view and dashboard on several parameters such access, user types, user profile, user log, top viewed content, etc.

i. Personalized Dashboards should be available to deliver relevant, easily understood real-time data to NFAI/ NFHM management. NFAI users should be able to access to personalized dashboards that deliver easy-to-understand summary information on a regular, scheduled basis. The module should enable exception reporting should alert the users to unexpected events and scenarios that require action. In addition, the dashboard should generate downloadable reports based on data filters. Discover, visualize, and explore actual business processes and customer experiences.

ii. Gain visibility into end-to-end business processes by analysing data streams to identify patterns, outliers, and trends.

iii. Analysing data to identify Customer preferences are expectations, likes, dislikes and patterns that drive customer purchasing decisions.

iv. Analysis should complement customer needs in explaining customer behaviour.

v. Real time search/query and faster reporting on data from multiple sources.

15.4.3. Collaboration: A collaboration platform needs to be setup between NFAI, research scholars, general public, DCP projection units, external agencies to ensure a communicative, collaborative, and cooperative workflow. The core features of a collaboration platform may include:

i. A shared workspace platform, acting as a digital "home base" for employees
ii. Customizable user groups
iii. Customizable personal dashboards on that shared platform
iv. File or document management
v. Chat or discussion forums
vi. Third-party app integration including OTT
vii. Workflow routing as per need (dynamic)
viii. Team member tagging capabilities

15.4.4. Audit Trail:

i. An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and this feature will log all the user transactions across all the application modules with date-time stamps, creator, editor, and details of data added/changed/deleted. This will complement the security & integrity of the eco-system. source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.
ii. Track the addition/modification/deletion of data in a data repository.
iii. View or create a report of all user access profiles, user id login and logout times over a specific period
iv. View or create a report of functional usage by user ID of system activity over a specific period, e.g., list the number of times each type of system activity (report, query, accession, etc.) was accessed on a certain day by a user
v. View or create a report by system activity on user access over a specific period, e.g., for each system activity (report, query, accession, etc.) list each user who accessed on a particular day.

15.4.5. Localization: this will provide localization e.g., support for local languages using Unicode.

i. The proposed application should support the process of designing a software application such that it can potentially be adapted to various languages and regions without engineering changes. It should support Localization where the process is of adapting internationalized software for a specific region or language by adding locale-specific components and translating text.

15.4.6. Notification: notification & alerts over email and/ or SMS etc. will be offered across all the applications.

i. The system should have a comprehensive logging / audit and exception handling mechanism
ii. The proposed solution should have the ability to show recent faults and errors and be able to display recent error messages and exceptions handled
iii. Should be able to generate alerts and email notifications to select groups.
iv. Should be able to generate OTPs required during user registrations for media access
v. Should have email integration capabilities and shall accommodate event or criteria driven email notification to select user group.
vi. Should support configurable email notifications in case events like document deletion, document access removal, documents submission for approval and generate of predefined alerts and notifications for various activities

15.4.7. Security Information and Event Management

i. Solution must have capability to pull logs for monitoring. Raw data flows into solution from a variety of sources, including logs, system metrics, and web applications
ii. Solution must be three layered architectures to achieve modularity, separation of data, data access control, scalability
    - Log/metric collection & sending agents
    - Central/hub collection, store, and indexing layer
    - Dashboard, search, and Analytics layer
iii. Solution must have lightweight agents for sending data to collection, store & indexing layer

iv. Solution must have data ingestion process by which this raw data is parsed, normalized, and enriched before it is indexed

v. Once indexed, users can run complex queries against their data and use aggregations to retrieve complex summaries of their data.

vi. Solution must have search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured.

vii. Solution must support REST APIs, distributed architecture, speed of integration and scalability

viii. Solution must have distributed capabilities/modules for data ingestion, enrichment, storage, analysis, and visualization

ix. Solution must enable creation of powerful visualizations of data, share dashboards

x. Solution must have server-side data processing capability that ingests data from multiple sources simultaneously, transforms it, and then sends it to Collection, store & indexing layer.

xi. Solution must dynamically ingest, transform, and ship data regardless of format or complexity. Derive structure from unstructured data with grok, decipher geo coordinates from IP addresses, anonymize or exclude sensitive fields, and ease overall processing.

xii. Shall have ability to index many types of content mean that it can be used for a number of use cases by integrated required data sources:

xiii. Solution must enable logging and log analytics

xiv. Solution must support a variety of inputs that pull in events from a multitude of common sources, all at the same time. Easily ingest from logs, metrics, web applications, data stores, and various Cloud services, all in continuous, streaming fashion.

xv. Must orchestrate ingest-to-visualize experience with popular data sources. With the power to instantly deploy ingestion pipelines and sophisticated dashboards, your data exploration starts in minutes.

xvi. Solution must correlate a set of keys (names of fields or properties) with their corresponding values (strings, numbers, Booleans, dates, arrays of values, geolocations, or other types of data)

xvii. Solution must have indexing technology allow very fast full-text searches and make document data searchable in near real-time.

xviii. Must be based on common schema which defines a common set of document fields for data ingested and support uniform data modelling, enabling to centrally analyse data of all kinds with both automated and interactive techniques.

xix. Must have data visualization and management tool that provides real-time histograms, line graphs, pie charts, maps and canvas which allows users to create custom dynamic infographics based on their data, and maps for visualizing geospatial data.

xx. Solution must be based on big data platform.

xxi. Solution should detect advanced threat & Anomalies by using machine learning.

xxii. Real time monitoring and alerting to stop threats faster

xxiii. Incident response and investigation to address and manage potential breach

xxiv. Solution should monitor user activity on real time to detect and alert any anomalous behaviour .

xxv. Threat intelligence should be available to capture threat feeds on real time.

xxvi. Advanced security analytics by leveraging machine learning to identify hidden threats.

xxvii. Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business

xxviii. The solution must be able to assign any arbitrary risk score to any data point or fields, example, username, host name, location etc.

15.4.8. User Behavior Analytics

i. The solution must be able to detect insider threats using purpose-built models or algorithms.

ii. Should provide context around the threat via anomaly correlation and visual mapping of stitched anomalies over various phases of the attack lifecycle.

iii. Should increase Security efficiency with rank-ordered threats and supporting evidence

iv. Should support bi-directional integration with SIEM for data ingestion, correlation, incident scoping, workflow management and automated response.

v. SIEM, UBA & BI platform should be delivered by single/multiple OEM as deemed appropriate by the MSI.

vi. Should incorporate Single Reporting console to monitor and manage SIEM, UBA & BI Platform.

vii. Should provide uniform data platform to ingest all types of standard and non-standard logs from any source.

viii. The solution should provide compliance use cases to identify usage of insecure, legacy, and deprecated encryption algorithms being used by servers on the network.

ix. The solution should be able to detect Unknown or encrypted malware, insider threats, policy violations.

15.5. Enterprise Services Bus (APIs)

The entire solution architecture & its components need to be connectable from application layer as well as database layer. Each of the components needs to be connected to homegrown systems & upcoming external systems - such as the RFID based physical asset tracker or external OTT platforms. APIs (REST, etc.) or SDKs needs to be available for the entire architecture. Creating And maintaining an enterprise level connectivity platform, along with sample codes in various languages, sample SDKs – to be a part of the scope for the MSI.

15.6. Data

15.6.1. The MAM based storage & the rest of the solution is expected to generate massive amounts of structured & unstructured data. The system should be able to decipher the most from these data sets.

15.6.2. Starting from features such as AI & ML based data cascading, categorization, advanced search, this data should be able to manage most of the advanced need for analysis, insights & decision making, etc. Every dataset to has its own dynamic (AI & ML based) data retention & management policy. Every data irrespective or

media or non-media should be 100% lossless for any period. Migration, upgradation, or any sort of maintenance needs to be ensured for 100% quality & hygiene of system and data.

15.6.3. With the data layer an entire data lake is resembled. Any sorts of data (SQL, NO SQL, content, etc.) should be stored in the data layer. The idea is to retain all data, faster insights, enormous horizontal & vertical scaling.

15.7. Security & Access Control

Security is one of the utmost important aspects envisaged in the entire solution design of NES. All key dimensions like, authentication, sessions management, context sharing and role-based access control, should be an integral part of the NES architecture. There should be a provision of logging into the system through Internet as well as through intranet. NES should comply with all requirements of security, reliability, and non-repudiation as per Government of India guidelines.

The Security will be implemented in an all-pervasive manner which will cover all the layers of the eco-system. Following are some of the Security Functionalities expected from the system:

15.7.1. The system should have role-based access control

15.7.2. System should support Single Sign On

15.7.3. Communication based on SSL and relevant encryption

15.7.4. The system should have role-based streaming/ download restriction mechanism.

15.7.5. Protection against phishing, DOS, identity theft etc. should be part of the solution

15.7.6. The security should work cohesively with the Audit Trail system and should be able to leverage the notification functionalities.

15.7.7. The infrastructure level security mechanism (e.g., IPS, Firewall) should work in conjunction with the Application-Level Security System.

15.7.8. The key security requirements are mentioned below:

15.8.1. Identity & Access Management

The key requirements for Identity and Access Management are mentioned below:

i. The solution should be capable of uniquely identifying all users of the system and their activities, providing user access rights to system and data which will be in line with the defined functional requirements

ii. The user account management component of the solution should address requesting, establishing, issuing, suspending, modifying, and closing user accounts and related privileges, with a proper approval process
iii. The system should be able to perform regular audits and management reviews of all accounts and related privileges
iv. Should provide Single Sign-On facility, support Mobility, Fraud Prevention/Detection capabilities

15.8.2. Access Control

i. NES must ensure that the access rights of all stakeholders and users to information and information processing facilities shall be removed upon termination of their employment or adjusted upon change.
ii. MSI will create single profile/user database which will act as a master source to provide role-based access to all users.
iii. Solution should have the capability to define access based on time of day, day of week or by group or user defined access, display the last login status (successful/ unsuccessful, time) to the user.
iv. The solution should have the capability to delegate the role if required for a set of specified users as decided by NFAI during the course of the project.
v. The solution should be able to deploy and configure password policy as approved by NFAI
vi. The solution should have the option of blocking multiple sessions for the user.
vii. Users should not be able to browse past their user role rights. User should not be able to access an unauthorized page by entering the location into the URL.
viii. The application should support role-based access control to enforce separation of duties.
ix. The application should not store authentication credentials on client computers after a session terminates.
x. Users' activity should not be cached when handling sensitive information.
xi. Any information stored within cookies must not be disseminated to third parties without the users' consent.

xii. NES should be able to deploy and configure password policy as approved by NFAI. The password policy should include the complexity requirements, password expiry, masking of password when typing, authentication for password reset etc.

xiii. NES should ensure secure session management in the application – invalidating session when user logs out, session time out, placing logout on all links that require authentication, protecting session ID, changing session ID etc.

15.8.3. Authentication, Authorization and Single Sign-on

i. The MSI will need to ensure provision for authentication using digital certificates as per the government of India guidelines. NFAI will however reserve the right to procure digital certificate for the end users whenever required.

ii. Users must be provided 'single sign on' functionality for the entire NES and modules deployed.

iii. The system should provide the single sign-on facility i.e., once any users credentials are verified, he/she should be able to navigate through all the modules and functionalities of the integrated application, to which that User is authorized to access.

iv. The portal security solution must examine all traffic to all resources of NES and all access attempts to the portal or directly to any resource managed/accessed by the portal, should be intercepted by the security solution, and examined for authentication and authorization requirements defined for the resource.

v. Any access to end users to database should only be via application/portal authorization

vi. All types of users shall enter the solution using appropriate secured authorizations.

vii. Portal should validate the mobile number and email address provided by each registrant by means of sending confirmation passwords via both SMS and email.

viii. UI interface as well as existing rights be managed through the same. The details of any change in the module should be captured in the Audit Trail of the application. Also, there should be facility to assign/ modify/ deactivate/delete rights globally for the desired Groups within the system.

15.8.4. Application Security

i. NES must comply with the Application Security Plan and security guidelines of Government of India as applicable and Information Security Management System (ISMS) – ISO 27001:2013 standards.

15.8.5. Data Encryption, Object Signing & Database Roles

ii. All the interfaces between various applications and user are encrypted using appropriate protocols (such as HTTPS, IPsec etc.), algorithm and key pairs.

iii. NES should support 128-bit encryption for transmission of the data over the Internet.

iv. Encryption of attachments (documents) shall be compliant to published Government of India standards.

v. Proposed solution must be secured to both internal and external parties (such as through password encryption)

vi. NES should use electronic signatures, data encryption and other methods to assure the authenticity of transaction and other relevant data

vii. NES should treat the following events as security incidents: unsuccessful log-on, intrusion detection, malfunctioning of encryption facility, etc.

viii. Database server should support encryption of sensitive data

ix. MSI should ensure creation of incident logs

x. MSI should make provisions for secure content management on the portal.

15.8.6. Privacy Policy & Notice

i. MSI should develop a privacy policy to be posted on the web portal in due consultation with NFAI. Privacy policy should be in line with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

ii. MSI should ensure compliance to the IT act 2008, Amendment 2008 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

15.8.7. Design and Implementation Aspects

The MSI shall be responsible to create and manage design, development, customization, and implementation of the proposed solution with approval from NFAI. Proposed solution should comply with all the functional & architectural requirements mentioned above.

15.8.7.1. Requirement Study

The MSI shall perform the detailed assessment of the Solution requirements as mentioned in the sections above. Based on the above, MSI shall prepare the Functional Requirements Specifications (FRS) and the System Requirement Specifications (SRS) in consultation with NFAI and other concerned representatives. While doing so, MSI is expected to do following:

i. Communicate with stakeholders and/or their designated agencies and bring in domain & technical experts during the study.
ii. Translate all the requirements mentioned in the document into System Requirements.
iii. Follow standardized template for requirements capturing. The templates have to be submitted to NFAI for approval prior to start of the requirement study.
iv. Present highlights of the SRS to the stakeholders.
v. Maintain traceability matrix from SRS stage throughout the entire development & implementation lifecycle.

15.8.7.2. Design

The MSI shall be entirely responsible for the design and architecture of the system implemented to satisfy all requirements as described in this document including sizing of the required hardware. Solution architecture description provided in the RFP is for reference only and the MSI is expected to design, build & implement the best solution based on the requirement gathered by the detailed requirement study.

i. The system architecture should be based on open industry standards and protocols
ii. The system shall be designed to be scalable, easily extensible, and interoperable.
iii. The system should be flexible to cater to changing business, industry, and compliance requirements.
iv. The solution should be designed & developed taking into consideration security, performance, efficiency, and maintainability.

v. The ownership of the product licenses would be with NFAI. All the licenses used as building block of NES should be mentioned clearly.

vi. The products which would be part of the Solution must be the latest commercially available versions.

vii. Products must be supported in terms of upgrades, bug fixes, functionality enhancements and patches to cater to changes to statutory requirements by their respective developer organization for a period of not less than five (5) years from the date of procurement

viii. Upgrades should be free of cost and upgrade process should be non-disruptive.

ix. The integrated solution design should enable integration of both internal and external applications and services. Integration should be based on open standards.

x. As NFAI is a custodian of the digital assets, MSI needs to take this into consideration to protect the data against corruption, theft, or destruction.

xi. Data should only be accessed through application/interfaces for upload, create, update, and delete. There should not be any direct access to the data layer for users

xii. MSI shall provide strategy to maintain data security for presentation & application Layer.

xiii. MSI shall provide strategy to maintain data security of the database, file systems, Common Services & applications.

15.8.7.3. Development

The MSI shall carefully consider the scope of work and provide a solution that best meets NFAI's requirements.

i. The MSI will be responsible for supplying the application, licenses, database and related software, integration tools, along with the source code and installing the same so as to meet NFAI's requirements mentioned in various sections of this RFP. The application if part of the entire solution should be seamlessly integrated with the platform.

ii. The MSI shall at regular intervals perform audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. Any non-compliance should be immediately reported. Any penalty due to non-compliance should be borne by the MSI.

iii. MSI shall implement a system for monitoring SLAs. The MSI shall ensure that the system addresses all the SLA measurement requirements and calculation of applicable penalties

as indicated in the RFP.

iv. The MSI shall provide all relevant documentations along with the developed components.

15.8.7.4. Testing

i. The MSI shall provide a comprehensive Test Plan consisting of Traceability matrix, Test Cases with mutually agreed parameters & test criteria. Test plan should be provided for prototype test, unit tests, system integration tests (SIT), stress tests, security Testing and final user acceptance test (UAT). The MSI is responsible to identify and inform the NFAI regarding testing requirements and impacts as well as test data.

ii. MSI shall provide complete support to NFAI team or their representatives at the time of user acceptance testing. It would be MSI's responsibility to ensure that all issues raised during UAT are closed and signed-off from competent authority.

iii. The MSI is required to submit a certificate from the OEM to certify the implementation as well as provide support for the entire contract duration. The entire support cost from the OEMs should be clearly stated in the proposal and included in the commercial bid. There must not be any additional charges/cost raised to NES with regard to OEM support, for the entire duration of the project.

15.8.7.5. Hand-holding support

MSI shall also provide hand-holding and requisite training support to NFAI personnel for a minimum period of 3 (three) months before the Go-Live of respective application. Post the Go-live date, following is the schedule of training to be conducted by MSI:

i) First Training: Three months post completion of second year (from the Go-live date)

ii) Second Training: Three months completion of fourth year (from the Go-live date)

For each of the trainings mentioned above, MSI shall provide requisite no. of people for hand-holding support at NFAI. MSI shall prepare a detailed training plan and get it approved from NFAI before start of the training.

15.8.7.6. Go-Live Preparedness and Go-Live

i. MSI shall consult with NFAI and prepare the detailed plan for Go-Live.

ii. The MSI shall discus with NFAI and subsequently prepare the criteria for Go-Live and the timelines for the same.

iii. UAT report (issue closure report) along with the resolution of issues is to be signed off

before Go-Live.

iv. MSI shall ensure that Go-Live criteria as mentioned in Go-Live plan is fulfilled and take approval from NFAI team on the same.

v. Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan

15.8.8. LTO Tape Management

15.8.8.1. MSI, after due consultation and approval from NFAI, shall retrieve contents as specified in Chapter 2: Section 1 from LTOs.

15.8.8.2. It will be MSI's responsibility to ensure adequate upkeep of LTOs and security of the content therein. This responsibility is for the LTO tapes containing the access files (HD, mp4, Apple ProRes, DCP etc.)

15.8.8.3. Post the above set of activities, NFAI will keep and maintain the LTOs (containing the raw files i.e., DPX and wav files).

15.8.8.4. It will be NFAI's responsibility to ensure that the LTO tapes (containing raw files, i.e., DPX and wav files) are stored in the physical location in an easily accessible and systematic manner, post due consultation and approval from NFAI.

15.8.8.5. The cost towards back up storage of copies of LTO tapes in the physical location will be borne by the NFAI.

15.8.8.6. The location of the Tape Library should be in the physical premises of NFAI in the Media Ingestion Room. The secure upkeep of LTO Tape library and Media Ingestion room shall be responsibility of MSI.

15.8.8.7. The storage facility should be as per standards and norms required for the LTO Library.

15.8.9. Security Audit

It is the responsibility of the MSI to get the Security audit, Application Audit & Vulnerability and Penetration Test of the web application, NFAI website, portal, NFAI Enterprise Solution done with a third-party agency which is CERT-IN empaneled security auditor. MSI would be required to share the complete details of the audits with the along with copies of all communication and bug reports / removal, written or otherwise. MSI needs to update the system in response to any adverse findings in the report, without any additional cost to NFAI. NFAI may also depute auditors to conduct security check/ vulnerability test/ penetration test.

15.8.10. General Technical Requirement

The MSI shall be responsible to adhere to all the technical requirements as mentioned in this section below.

15.8.10.1. The NES Solution should be web-based multi-tier application having centralized database and application server.

15.8.10.2. The Solution should be compatible with various open standards and technologies and should not restrict NFAI in using the Solution data for any other applications.

15.8.10.3. The system's development environment and databases should not restrict NFAI from using the application or data in any future applications.

15.8.10.4. The Solution should support bilingual (English and Hindi) and should be UNICODE compliant supporting Screens, data entry, search facilities, reports etc.

15.8.10.5. Should be compatible with any of the Microsoft, Linux and UNIX based operating systems.

15.8.10.6. Should support interoperable, portable, and scalable applications, services, interfaces, data formats and protocols.

15.8.10.7. The solution should be browser, platform independent.

15.8.10.8. The portal shall be accessible through mobile and other handheld devices like iPad; tablets etc. and the pages shall adjust suitably as per the device

i. Appearance Requirements

a. The Solution should have Pull down menus, command buttons, short-cut keys, and pop-up windows, and use other navigation aids wherever possible to make the product efficient and easy to use.

b. The Solution user interface should make use of the horizontal and vertical scroll bar feature wherever needed, depending on the layout of the window.

c. The Solution should have an ability to configure restricted and mandatory fields wherever relevant.

d. The Solution should use standard drop-down lists wherever possible for standard values to be selected by the user.

e. The Solution should have the functionality, but not limited to the following.

- Define user groups.
- Define users.

- Map users to group.
- Assign the users a role and privileges in the applications
- Give/ impose data-based access/ restrictions to the user's e.g., specific applications, plans, approvals, reports etc.
- Disable/re-enable modules within application.
- Define menus and attach such menus to users/ groups.
- Disable/re-enable users/groups from the system

f. The Solution should enable multi factor authentication with combination of hardware tokens, software tokens, etc.

g. The Solution should suspend the user in case of a specified number of unsuccessfully attempts to logon to the Solution and these suspended user IDs should only be reactivated by the system administrators.

h. The Solution should store all authentication credentials of users in an encrypted format.

i. The Solution should allow the administrators to 'forcibly' log out users, in case needed.

j. The Solution should maintain following categories of logs:

- Solution access logs.
- Solution health logs.
- Solution error logs.

k. The system should have an integrated audit log capable of recording, displaying, and reporting all transactions occurring in the system.

ii. Performance Requirements

The expected load on the system may be calculated based on the following:

a. The peak number of users (internal and external) using the Solution concurrently may be around 500.

b. The load design should also consider the Solution usage by external and internal users.

c. The average Solution response time (time taken for loading of a page) for users should not exceed three seconds. The MSI shall provide the tools and mechanism for capturing and reporting the response time.

d. Solution should be upwardly scalable in the event of increased usage of the system or inadequate performance or new requirements.

e. The Solution should utilize a database schema and design that is capable of handling current and future workload as defined above.

16. Cloud Hosting

16.1. MSI is required to arrange for cloud-based hardware infrastructure to host the proposed Enterprise solution. Infrastructure will include server, information security, network, storage, secured access of the solution through the internet. Cloud Service offerings of CSP should be certified by MeitY for compliance to the published standards and guidelines.MSI shall configure the entire cloud infra as per the requirement of NFAI and deploy the NFAI's Enterprise Solution on it. Any challenge related to deployment / upgradation / modification of application in cloud will be supported by CSP and will be the responsibility of the MSI.

16.2. MSI/CSP Shall operate and maintain the cloud infra 24 hrs.*7 days*365 days per year and resolve all incidents, problems defined in SLA.

16.3. For all the cloud services being quoted, the MSI has to ensure that all software being offered are genuine and comply with the licensing policy of the software OEM.

16.4. MSI Shall provide the cloud service offerings for a combination of the Deployment Models as IaaS, PaaS, SaaS.

16.5. The MSI would be responsible for provisioning of required IT infrastructure as IaaS, PaaS, and SaaS as per NFAI application hosting requirements.

16.6. The proposed landscape for the deployment of Application solution is

a. Test and Development (T&D)
b. UAT
c. Staging
d. Production
e. Others if required

16.7. The NES shall be deployed on the VPC.

16.8. Each of the environments mentioned above shall be logically isolated.

16.9. The CSP/MSI is required to have IP v6 support.

16.10. The CSP/MSI shall be responsible for provisioning and deployment of required compute infrastructure virtual machines, cloud native managed services, storage, security component, Backup etc. for hosting NFAI applications. The indicative IT infrastructure requirements are mentioned in separate section.

16.11. The CSP/MSI shall be responsible for provisioning and deployment of IPSEC connectivity over Internet between cloud setup and Application service provider as well as NFAI to enable access to manage the cloud services. IPSEC at NFAI end and at Application provider end will be provided.

16.12. The CSP/MSI will be responsible for provisioning and deployment of requisite network infrastructure services such as firewall, VPC, ACLs and Load Balancer to ensure accessibility of the cloud services as per defined architecture.

16.13. The CSP/MSI will be responsible for provisioning of UDP File Acceleration Services/ appliance at NFAI for data transfer.

16.14. The CSP/MSI will be responsible for ensuring data is encrypted at REST and in motion.

16.15. The CSP/MSI shall configure DNS to provide access the URLs (Public and Private) as per NFAI requirements.
16.16. CSP/MSI is required to propose the cloud native architecture wherever applicable in the propose solution. The propose solution shall be independent of any platform / OEM and it can be migrated to any other platform without any customization.
16.17. The CSP/MSI shall configure the role base access of all the users who need access on production, Staging, UAT and other environments. Complete access management of hosted application and services should be role based and reports shall be available to NFAI.
16.18. Admin access to cloud components should be secure and only be accessible from VPN.
16.19. The CSP/MSI shall ensure that all access, audit, system and security, API gateway logs should be stored for audit purpose. NFAI will take decision to finalize the archive policy.
16.20. CSP/MSI Shall deploy and configure security components as per solution defined by NFAI.
16.21. CSP/MSI shall submit the HLD/LLD to NFAI before provisioning the IT setup on cloud and should submit the as-Is post implementation.
16.22. The cloud service provisioned and deployed by the CSP/MSI shall be scalable and allow NFAI to add/reduce cloud resources on demand basis whenever required.
16.23. The CSP/MSI shall provide a portal that allows automation of cloud recourse management, tracking, and optimization advisory.
16.24. CSP/MSI ensure the UAT, and Staging cloud should scale down whenever NFAI is not performing the testing.
16.25. The solution needs to provide the ability for NFAI IT Administrators to access the cloud environment to view the metering, billing, and services available on cloud.
16.26. CSP/MSI Shall provision and configure the backups for the data of VMs as per the policy approved by NFAI.
16.27. CSP/MSI Shall provide the portal access to log the tickets for incidents and problems for NFAI users and NFAI application provider.
16.28. CSP/MSI Shall assign technical manager to NFAI (NFAI's authorize application provider) for critical Incidents to on board the technical team to fix the issue on priority as per defined SLA.
16.29. CSP/MSI Shall provide the cloud native tools to monitor the performance of IT setup including the compute, memory, disk, IOs bandwidth, application parameters and provisioned services.
16.30. CSP/MSI Shall configure dashboard to monitor the performance of NFAI cloud Infrastructure, as per the requirements of NFAI.
16.31. CSP/MSI shall also customize the dashboard as per NFAI requirements, from time to time.
16.32. CSP/MSI shall submit all the configured policies of Anti- DDos, firewall, load balancer, WAF and other security components to NFAI and update the document wherever policy changes.
16.33. CSP/MSI shall provision and deploy the cloud services jointly with NFAI admin team in NFAI office and provide all access to NFAI team or authorized partner.
16.34. CSP/MSI shall provide the support to NFAI authorized application partner to deploy the application on provisioned cloud.

16.35. The MSI shall conduct vulnerability and penetration test at their cost (from a third-party testing agency which should be CERT-IN empaneled and approved by NFAI) on the Cloud facility every 6 months and reports should be shared with NFAI. The MSI needs to update the system in response to any adverse findings in the report, without any additional cost to NFAI

16.1. Security and Statutory Requirements

A. The CSP services need to be certified / compliant to the following standards based on the cloud requirements:
    1. ISO 27001 - Cloud services should be certified for the latest version of the standards.
    2. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.
    3. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in Virtual Private clouds.

   The CSP/MSI shall comply or meet any security requirements applicable to CSPs published (or to be published) by Ministry of Electronics Information and Technology (MeitY), Government of India

   or any standards body setup / recognized by Government of India from time to time and notified to the CSPs by MeitY as a mandatory standard.

B. The CSP/MSI shall meet all the security requirements indicated in the IT Act 2000 the terms and conditions of the Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC.

C. The CSP/MSI shall comply with the requirements of proposed Data Protection Act.

D. All the NFAI's data stored in cloud, should remain hosted in India and it should not go outside India. This is applicable for On Cloud DC as well On Cloud DR.

E. CSP/MSI shall propose cloud services available from India location only.

F. CSP/MSI shall ensure that whenever NFAI asks to delete any data from cloud then data should be deleted in all forms.

G. CSP/MSI Shall have provision for the below security components to secure the environment
    1. DDos protection
    2. Next Generation Firewall with capabilities to identify signature based and behavior-based anomalies
    3. Anti-virus and HIPS (for virtual Machine)
    4. Data Encryption at rest and in transit
    5. SSL off-load/ Data protection
    6. Web Application Firewall (WAF)
    7. Basic SIEM and Security Reporting
    8. Network Zoning

9. Others (If required)

16.2. Migration

A. Technologies are changing very fast and NFAI would be needed to upgrade the cloud service time to time. CSP/MSI Shall plan the migration (within the same cloud) on new technologies available on cloud and ensure the error free migration of running workloads, Databased and other components based on decision taken by the NFAI.
B. MSI/CSP Shall not charge any extra amount other than charges applicable to new services. MSI/CSP Shall submit the plan for migration after discussion with NFAI and third-party application vendor authorized by NFAI.
C. Provisioning of new services and migration of existing services would be responsibility of CSP/MSI. CSP/MSI would ensure the business downtime should be minimum

16.3. Provisioning Cloud services for additional quantities at proposed rate

The rates offered for cloud services must be valid for entire contract/project duration. No variation in these quoted rates shall be allowed during this period. NFAI will have liberty to order additional cloud service items, at the rates offered in the commercial bid. NFAI reserves the right to scale down and scale up the Cloud IT infrastructure. The payment would be made only on the actual usage of the Cloud IT infrastructure as per the rates provided by the MSI in their Commercials and as per the payment terms mentioned in the RFP.

16.4. Project Management and Governance

The CSP/MSI shall provide the details the governance framework in its proposal and can propose its own governance structure as part of response to this RFP. The CSP/MSI's proposed governance model would be discussed between MSI and NFAI at the time of on boarding. The final governance model shall be approved by NFAI.

CSP/MSI Shall appoint one Project Manager and he/she would meet formally on a monthly basis covering, at a minimum, the following agenda items:

1. Project Progress
2. Incidents and Problems report
3. Issues and concerns
4. Performance and SLA compliance reports
5. Unresolved and escalated issues
6. Change Management - Proposed changes if any
7. Project risks and their proposed mitigation plan
8. Discussion on submitted deliverable

9. Timelines and anticipated delay in deliverable if any
10. Delays, if any – Reasons thereof and ways to make-up lost time
11. Any other issues that either party wishes to add to the agenda.

16.5. Project Monitoring and Reporting

CSP/MSI Shall submit the below defined reports by the first week of every month so that these reports can be discussed on monthly review meeting. These reports are indicative and NFAI may add more report as per requirements in operation phase.

CSP/MSI and NFAI mutually will form a steering committee that will monitor the progress of the project during implementation and in operation stage. This committee will meet a periodic interval to ensure smooth functioning of the project

1. Incidents reported on monthly basis.
2. Incident resolution timelines with dates.
3. List of all VMs and their CPU performance average, Min, and Max.
4. List of all VMs and their Memory performance average, Min, and Max.
5. List of all Security appliances and their performance.
6. Bandwidth performance of all links.
7. List of storage disks and their IO performance.
8. SLA report as defined in section "Service level Agreement".
9. List of changes planned, Change approved and implementation.
10. Performance of Databases
11. Performance of Cabernets containers
12. Performance of Security components
13. Security solution/SIEM Reports
14. DDos Reports
15. Others if required

16.6. Reporting for Infrastructure at Media Ingestion Room

This is to communicate the compiled information as outcome of any activity related to the Media Ingestion operations. It is important that these documents are accurate, objective, and complete according to its purpose as this is the only relevant factor used for referencing.

a. Media Ingestion Activity Report – CR (Change Request) can be monitored quarterly, and annually.

b. PM (Preventive maintenance Reports) – This should be submitted quarterly. This ensures proper maintenance has been done.

c. Incident Report – It is required to monitor every incident to prevent recurrence.

d. KPI Report – This is to monitor all targeted activities. Can be monitored monthly, quarterly, and annually.

16.6.1. Quarterly Reports

Consolidated component-wise Media Ingestion Room infrastructure availability as mentioned bellow has to be submitted to all the stockholders involved in the project in hardcopy as well as in softcopy.

1. Component wise IT infrastructure availability.

2. Log of preventive / scheduled maintenance undertaken

6. Log of break-fix maintenance undertaken

7. Summary of attendance of MSI's staff at the Media Ingestion Room.

17. NFAI Web portal – Design, Hosting, Operations & Maintenance

17.1. Hosting, Maintain and Manage

The Selected Master System Integrator shall be responsible for the following:

i. MSI shall be responsible for hosting of NFAI website on cloud where NES is hosted.

ii. Management of the existing NFAI official website as well as design and build independent modules for the existing official website (www.nfai.gov.in) as per the requirements of NFAI. The source code of the existing website shall be provided by NFAI. The MSI will ensure that the good practices and GoI (Government of India) guidelines for Software development listed below as well as localization are used during the upgradation of existing design, development/customization, and implementation and maintenance phase.

Sr. No	Name of guideline	Description	Requirement
1	Localization & Language Technology Standard	Best Practices for Localization of e-Governance applications in Indian Languages for web and mobile applications	Mandatory
2	Policy on Adoption of Open-Source	Adoption of Open-Source Software in all e-Governance systems implemented	Mandatory

Sr. No	Name of guideline	Description	Requirement
	Software for Government of India	by various Government organizations, as a preferred option in comparison to Closed Source Software	
3	Guidelines for Indian Government Websites (GIGW)	These Guidelines address the entire lifecycle of a website, web portal/application right from its conceptualization to design, development, maintenance, and management	Mandatory
4	Web Content Accessibility Guidelines (WCAG) 2.0	The WCAG documents explain how to make web content more accessible to people with disabilities	Mandatory
5	eGovernance Standards	Website should be in compliance with eGovernance Standards of Government of India	Mandatory
6	Interoperability Framework for e-Governance (IFEG)	Technical Standards for Interoperability Framework for e-Governance (IFEG) in India Version 1.0 or higher	Mandatory
7	MDDS	Demographic Standards, Character Encoding, Font Standard, eGov.BIDS	Mandatory
8	eSAFE	eSAFE-ISF01, eSAFE Framework (and associated documents) or higher	Mandatory
9	Digital Signatures	Digital Signatures in e-Governance software	Mandatory
10	Open standard Framework	Open Standards for e-Governance, Framework for Mobile Governance	Mandatory
11	Technology stack	Details of the website such as Operating System, Database used, Web Servers used, Data Storage required, architecture, functionality, framework used etc.	Mandatory
12	STQC	Security audit to be performed through CERT-IN empaneled agency.	Mandatory

iii. Any new module / page development must be done with a platform, cloud neutral technology with independent / flexible technologies

iv. MSI shall provide all the 3rd Party Applications or APIs required for the systems at its own cost.

v. MSI shall migrate developed application to NFAI's cloud server and then perform STQC for website

vi. Develop application to support integration of Google Analytics or any other 3rd Party site analytics application

vii. MSI shall provide all the resources necessary for completion of the project including team of System architect, Project manager, software developers, testers/QA, Business Analysts, network engineer, any software required, language translator (English to Hindi) etc. NFAI shall provide necessary content to the MSI as and when sought.

viii. MSI shall allocate minimum One (1) fulltime resource on Site at NFAI Phase 1 office, however on critical issues resolution offsite help must be extended.

ix. Maintenance of the developed application shall also be part of the scope of the MSI during warranty period.

x. Bug tracking tool to be provided to purchaser with at least 3 user login credentials. The cost associated with the tracker would be borne completely by the MSI.

xi. Integration with the NFAI portal or any other NFAI applications existing at the time of development. There shall be provision for Hyperlinks for other NFAI applications

xii. The MSI shall understand the requirements and propose a best-suited solution meeting the industry standards, which helps in meeting the specific requirements of NFAI.

xiii. The software development and UAT should be performed on MSI's server and it must be hosted on cloud at his own cost.

xiv. When the tested software is deployed on Virtual Private cloud, there should be a round of testing done before Go-Live.

xv. NFAI will bear the hosting cost for Server for production servers in cloud.

xvi. Coordinate and provide necessary support for acceptance testing and systems audit (functionality, process, performance & security controls) to be performed.

xvii. MSI should conduct security audit and certification or engage a suitable neutral and technically competent third-party agency or agencies for conducting audit and certification, once the system implementation is complete. The third-party agency must be Cert-in certified agency.

xviii. Security Audit should be done after all feedback implementation (UAT, Training feedback and Pilot Project) and before Go-live.

xix. STQC certification acquiring from cert-in-empaneled agencies is sole responsible of the MSI along with the Cost associated with it.

xx. Subsequent STQC certification would be based on prevailing MeitY, GOI guidelines. No additional cost for any subsequent STQC certificates would be payable to the MSI during the Contract period.

xxi. Implement necessary access security and data validation controls during the development of the software application; security from all types of unauthorized / malicious access such as hackers, malware, spyware, and Trojans etc. Adequate measures should be taken to prevent cross-site scripting, SQL injection, phishing, and session hijacking.

xxii. MSI would procure and bear the cost of SSL for website including Disaster Recovery (DR) sites.

xxiii. Preparation of necessary User and Trouble Shooting manuals; conducting training sessions for NFAI users, administrators, trainers shall also be part of the scope of the MSI.

17.2. Functional Requirements (Backend)

17.2.1. Common features to be considered for the website modules are provided as below:

1. The system should be able to generate or upload relevant content as required by NFAI.
2. The system should generate or upload all the document in the word/excel/pdf/design/drawing format, etc.
3. The system should generate the trail and log of entry done by user.
4. The system should not delete any entry if any kind of approval is given, or such entry is used in system.
5. The system should have provision of super administrator and a local office level administration to manage the software module as per the hierarchy and delegation of authority in NFAI from both frontend and backend.
6. Application should be capable of integrating with existing systems at the time of development. Details shall be provided during the requirement gathering stage
7. The system must support a configurable session timeout which forces a user to log back in after a period to ensure security.
8. Captcha authentication is required during the login to prevent bots from automatically submitting forms with SPAM or other unwanted content.

17.2.2. General Design Requirements (for NFAI website and any new module developments)

The MSI shall develop new modules in compliance to the following high-level design considerations:

1. The solution shall be based on the use of web application framework, web content management system backed by a database, to deliver the sites contents.
2. Use of at least 3 themes, skins, pages, and page layouts to change the presentation layer of the site quickly and effortlessly without impacting the content or the structure of the site without IT Intervention.
3. The websites solution shall provide rich user interface.
4. **Design Interface** - The content in web pages should be a mixture of text, images, downloads & videos (where needed) and have symmetry in look & feel based on Themes & Navigation strategy.
5. **Look & Feel** - The websites should be developed by using base strategy of themes so that each section of the websites has symmetry in look & feel based on NFAI's objectives and logo

6. All content in website should be distributed in sections and sub-sections. Each section and sub-section should carry specific content type and should have easy navigation within that section and other related sections
7. **Dynamic Updates** - The content in each section of the websites should be able to dynamically update without updating the entire page.
8. Creation of rich artwork and photo/video processing to augment the content and overall branding
9. There shall be provision of an easy-to-use administration interface to update the content with at least 2 defined users. It should preferably provide WYSWYG interface for users with content updation rights
10. Use of SEO friendly clean permalink structure and SEO Best Practices for portal design, structure, and content.
11. It shall provide accurate and fast search through the portal pages and data uploaded without having to tag metadata manually. It should provide search filters for search results generated.
12. The MSI shall pre-configure the portals or widgets to integrate with the back-end systems and if required and make them available in the catalogue for end users' selection preferably in a store like format.
13. It shall allow administrator and authorized users to create and deploy portals and widgets with other users.
14. Provision of Role Based Access (Admin, editor, facilitator General User, Power User, Backup User etc.)

17.2.3. Easy Navigation

The website should be designed in such a way so that user level navigation is easier. Links & sub-links should be grouped in two or three layers (as required) of Navigation on top or/and left side of the web pages. The navigation and landing page should meet the international web standards.

1. There shall be clutter-free navigation with good Internal Linking
2. The header and footer shall be Informative
3. The home page & key section landing page of websites should load in 3 seconds or less and all other pages in 5 seconds or less
4. The website shall help both users and search engines navigate the site easily by mapping hierarchical list of pages (with links) organized by topic
5. The website should support Omni Channel form factor and should do auto sizing while streaming of images and videos based on available network.
6. The content in all sections or information modules of respective websites shall be published with vertical Scroll navigation only

17.2.4. Administrator Control Panel

A web-based control panel is required to centrally administer the content, theme, navigation, design, sections, pages, users, and database(s) of the websites. The website administrator shall be able to manage the individual webpage of website. The admin shall be able to add/edit/update/delete the required information. The Administrator's control should have following features.

1. Generation of Reports for management to check website traffic details such as unique visitors, return visitors, country/origin, pages visited, bounce off reports, most visited pages, modules, schemes, content consumption patterns, device/OS reports, most searched scheme category, schemes, institutions, path flow etc.
2. The reports must be updated real-time with latest update of information
3. The panel should enable easy to do ad-hoc analysis with the ability to create customized dashboards
4. The panel should support collaboration with easy sharing of reports
5. The panel should have the ability to create virtual reports/dashboards
6. The panel should have the ability to share audience segments real-time with other delivery platforms such as Optimization engines, applications Management systems etc.
7. The panel should provide detailed link analysis for a page to understand the most useful/accessed links on a given page, including real time analysis & updates
8. The system shall allow websites administrator to delegate the administration function.

17.2.5. Management Information System

1. System should include Dashboards for Data Analysis. The system should have a DASHBOARD where the status of progress would be displayed in infographics as well in its details. The same should be able to get projected on an independent URL which may be projected or consumed by authentication applied.
2. Dashboard will be needed for data analysis for indicative fields like documents uploaded in each Institutes for e.g. (Tender and publications etc.)
3. The system should be able to generate reports in MS excel or .csv formats or PDF format or drawing format for the review by NFAI.
4. The system should be able to search and view the details.
5. System shall maintain archives as per the requirements of NFAI
6. System shall be capable of query-based reports

17.2.6. Search

1. The website users should be able to search within website. The search results should be based on access rights
2. The website should provide metadata and 'full text search' based on elastic search functionality and support indexing and rendering of content from standardized formats

like MS Office, PDF, and HTML etc. This search should be available in both Hindi & English languages as specified

3. For providing search functionality the website should comply within defined processes for defining metadata, managing metadata schema changes and master data changes.
4. Search must allow the archived content to be included (or excluded).
5. Advanced search facility based on multiple filters or parameters to search specific content should be provided.

17.2.7. Integration with existing services and Open APIs

1. The solution must be able to integrate with existing as well as envisaged e-governance applications, Mobile Applications, other Web Applications etc. as per requirements in future
2. The system should expose APIs to interact with the third-party systems to enable seamless integration with the third parties. This would enable to be future proof allowing for integrations with solutions that are not currently available with NFAI
3. The system should have ability to integrate with legacy databases.
4. The system should support for both native and hybrid mobile apps and other front ends connecting through APIs.

17.2.8. Security

1. The website solution shall provide role-based security features.
2. The solution shall inherit the access control rights imposed by the underlying application/database when integrating with enterprise application.
3. It is the responsibility of MSI to install security certificates like SSL 3.0.
4. The MSI shall conduct security audit of the proposed websites from CERT-IN empaneled agencies, at their own cost
5. The MSI shall provide audit, analysis, and reporting tools to track the websites system usage and shall be able to track, analyze and generate reports on areas like portal pages hit, portal usage, security violations etc.
6. The MSI shall ensure that the NFAI website to be Security Audited by the Cert-In empaneled Security Auditors or Government of India empaneled Security Auditors.
7. The Cost for Security Audit of website should be borne by MSI.
8. The MSI needs to update the website solution or system in response to any adverse findings in the report, without any additional cost to NFAI & ensure complete security audit done successfully.
9. NFAI may also depute auditors to conduct security check/ vulnerability test/penetration test.

17.2.9. Scalability & Extendibility

1. The MSI shall ensure that the website solution is based on a scalable architecture. It should be compactible for integration of existing as well envisaged modules.
2. The Solution shall support both horizontal and vertical scaling.
3. The Solution shall provide for expansion of data storage as needed to accommodate increased volume of database on approved Capacity Plans by NFAI.
4. The Solution should also make use of a distributed cache to enhance the scalability of the system.
5. The proposed web portals should be able to expose its services to third party Systems/applications with REST/SOAP services or APIs. The website applications should be able to integrate seamlessly with any other application.
6. The solution should extend its capability to easily integrate with existing Citizen Services of NFAI.
7. The website solution and content management system shall have a well-defined framework for extending the functionality of the core product, by adding more modules. This will enable NFAI to request an additional module or set of modules without impacting either the core CMS application or other modules already in service.

17.2.10. Data Migration

Data Migration in the context of this NFAI website manage & maintenance scope shall be to entail migration of required existing content and data. MSI is expected to provide following services, but not limited to:

1. Carry out the data migration from existing module(s) to new solution wherever applicable.
2. Develop a data migration strategy which explains the sanitization, enrichment, migration, and testing strategy.
3. If required, liaise with current support vendor and design data extraction tools. The MSI shall be entirely responsible for data migration, validation, and integrity check.
4. In cases the data is not available and has to be digitized from the existing records, the data entry and validation exercise needs to be carried out. The MSI will:
    - Create Data Entry Templates based on the requirements
    - Train the end users in data entry
    - Migrate the data from data entry templates
    - Data Validation of entered data by running scripts
    - In such cases, the NFAI officials will be responsible for data entry and validating the data and give a sign off on the validated data.
5. The MSI will have to import the required data from the existing website to new environment. The MSI will have to collaborate with the NFAI to get the missing information and validation of the information

17.2.11. Online Support

- MSI shall provide online support for user feedbacks. Separate email ID and phone numbers shall be setup by the MSI to provide online support to users wherever required.
- As a standard practice it is required that the MSI to provide a resolution Hierarchy and therefore an Escalation matrix to NFAI for L1, L2 & L3 support with proper email ID and Contact number.

17.3. Web Portal Hosting

1. The MSI shall notify the NFAI for any other system software patch updates; Client / application provider has to test the patches for application compatibility and intimate MSI to roll-out the same. Major patching / update which requires system downtime has to be informed well in advance and should be undertaken only after NFAI confirmation.
2. The MSI should provide adequate security framework to ensure the security of the web portal hosted on cloud.
3. The MSI shall ensure that a DR drill is required to be conducted every six months. Report of which shall be submitted to NFAI authorities twice a year.
4. The MSI should have a governance structure in place to report to NFAI 's team on monthly basis and the solution should allow downloading of standard and custom reports on the monitoring status and provide web-based monitoring tools for system user hits, traffic, bandwidth etc.
5. The managed services provider shall provide monitoring alerts on real-time basis on web-based console via email for firewall / Bandwidth usage
6. Vulnerability testing and reporting of the same must be carried out each regularly.
7. Search engine optimization activities must be conducted regularly to ensure NES web portal along with the official web site must be visible in the first few search results in the leading search engines at all times.
8. All Security Requirements like HTML/ SQL Injections, application of Stored Procedures etc. should be taken care of.
9. It is the responsibility of MSI to provide sizing of all the infrastructure for NFAI website including cloud hosting (for DC & DR site), for meeting all the requirements and SLAs of the RFP. In case it is found that additional infrastructure & applications are required for meeting the RFP requirement and the same has not been considered in sizing, MSI shall provide/host all such additional infrastructure/ applications at no additional cost to NFAI
10. The hosting shall include the following sizing (including but not limited to)
    - All compute infrastructure like web servers, application servers, database servers, etc.
    - Software Licenses (Database, Application, etc.)
    - Storage space on cloud
    - Backup Services (including filesystem and database)
    - Any other components required for functioning of the proposed solution

17.4. Change request Management for NFAI Web site

NFAI may at any time, give written order to the MSI to make changes for additional functionalities or develop new modules specifically required, but not falling within the general scope of this document. Change order/management procedure will follow the following steps:

- It is hereby clarified that any change requests coming in within the three months of post Go-Live period will be delivered by the MSI without any additional cost to the project.
- Any change request proposed by the MSI shall be considered by NFAI only when the efforts involved are greater than 10% and less than 25% of the total work order value / total value of corresponding stage as applicable.
- Efforts lesser than 10% shall not be considered under change request management and the Agency shall be required to do the required changes at no extra cost to the NFAI.
- The total change request cost shall not exceed 25% of the total work order value.
- **Identification and documentation of the requirement for the change**: The information related to the initiator, initiation date, Priority of the change will be documented by NFAI.
- **Analysis and evaluation of the Change Request**: The impact of the change in terms of the estimated effort changed schedule, cost based on the financial Bid and the items impacted will be analyzed and documented by MSI.
- **Approval or Disapproval of the change request**: NFAI shall approve or disapprove the change requested after discussion with MSI on the impact of the change.
- **Implementation of the change**: The change will be implemented in accordance with the agreed cost, effort, and schedule.
- **Verification of the change**: The change will be verified by NFAI on the implementation of the change request.

17.5. Annual Technical Support

As part of ATS, MSI shall:

- Maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance
- If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same should be done as part of ATS
- Should carry out any requisite adjustments / changes in the configuration for as part of the ongoing maintenance
- Regular and thorough backups of NFAI website so that it may be fully restored in case of any loss.
- Monitoring NFAI website functionality to ensure that everything is working as it should and provide updates when necessary.
- Front-end updates to HTML, CSS, and JavaScript.
- Assisting with downtime or performance issues by liaising with the web host provider.
- Training, consultation, advice, and guidance on the use of the website.
- Security protection against hackers from gaining access to your site.

17.6. Back up and Preventive Maintenance

MSI shall provide for backup management services (conduct regular backups and restoration, if required), of critical data and systems for NFAI website. The activities shall include:

1. Backup of operating system, database, and application as per stipulated policies.
2. Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
3. Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by NFAI or in case of upgrades and configuration changes to the system.
4. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
5. On-going support for file and Folder restoration requests.

MSI should define and indicate the preventive maintenance schedule and procedure. Any special tools/ instruments/ equipment's required carrying out the preventive and break down maintenance of the system offered should be clearly indicated and offered to NFAI by MSI at no extra cost.

17.7. Regular reporting

The MSI shall submit the reports on a regular basis in a mutually decided format. The MSI shall workout the formats for the MIS reports and gets these approved by the NFAI within a month of being awarded the contract. The following is only an indicative list of MIS reports that may be submitted to NFAI:

a. Monthly reports

- Component wise server as well as web / functionality availability
- Consolidated SLA / (non)- conformance report.
- Summary of component wise uptime.
- Log of preventive / scheduled maintenance undertaken
- Log of break-fix maintenance undertaken
- All relevant reports required for calculation of SLAs

b. Quarterly Reports

- All relevant reports required for calculation of SLAs
- The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by NFAI

The MSI will also provide any other report requested by the NFAI.

18. Service Level Agreement

18.1. This section describes the service levels to be established for the Services offered by the MSI to NFAI. The successful MSI has to comply with below-mentioned SLAs to ensure adherence to quality, security, and availability of service. The MSI should provide adequate tools required to capture the data for SLA verification and will submit the SLA reports on the quarterly basis to NFAI. Definitions

18.2. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during 24x7 timeframe. Further, scheduled maintenance time is planned downtime with prior permission of NFAI.

18.3. "Scheduled operation time" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the on-cloud data center and on cloud disaster recovery center will be 24x7x365.

18.4. "System or Application downtime" means accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the scheduled maintenance time and measured from the time NFAI and/or its employees log a call with the MSI team of the failure, or the failure is known to the MSI from the availability measurement tools to the time when the System is returned to proper operation.

18.5. "Availability" means the time for which the services and facilities are available for conducting operations on the NFAI system including application and associated infrastructure. Availability is defined as:
{(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%

18.6. "Incident" refers to any event / abnormalities in the functioning of the any of IT Equipment / Services that may lead to disruption in normal operations of the cloud, System or Application services.

18.7. "Response time" is the time interval between a cloud service customer-initiated event (e.g., logging of the request) and a cloud service provider-initiated event in response to that stimulus.

18.8. RTO (Recovery Time Objective): RTO designates the amount of "real time" that can pass before the disruption begins to impede the flow of normal business operations seriously and unacceptably. The system should have a maximum RTO of 4 hours.

18.9. RPO (Recovery Point Objective): RPO is the amount of downtime a business can tolerate. RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. The system should have a maximum RPO of 2 hours

18.1. Interpretation & General Instructions

18.1.1. The availability for a service will be the average of availability across the entire functionality of the platform rather than on individual component or functionality. However, non-compliance with performance parameters for infrastructure and system/service degradation will be considered for downtime calculation.

18.1.2. MSI shall provide automated tool to monitor and report all the SLAs mentioned in the subsequent sections.

18.1.3. The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. The MSI is expected to provide the following service levels. In case these service levels cannot be achieved at service levels defined in the tables below, it shall result in a breach of contract and invoke the penalty clause.

18.1.4. A Service Level violation will occur if the MSI fails to meet Minimum Service Levels, as measured on a Quarterly basis, for a particular Service Level. Overall Availability and Performance Measurements will be on a quarterly basis for the purpose of Service Level reporting. An "Availability and Performance Report" will be provided by the MSI on quarterly basis to NFAI in an approved format and a review shall be conducted based on this report. A quarterly Availability and Performance Report shall be provided to the NFAI at the end of every quarter containing the summary of all incidents reported and associated MSI performance measurement for that period.

18.1.5. The SLAs will prevail from the start of the Operations and Maintenance Phase. However, SLAs will be subject to being redefined, to the extent necessitated by field experience at the user units and the developments of technology practices globally. Payments to the MSI are linked to the compliance with the SLA metrics laid down in the tables below. The penalties will be computed and calculated as per the computation explained in this Section. During the contract period, it is envisaged that there could be changes to the SLA, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e., NFAI and MSI.

Following points outlines the key service level requirements for the system, which needs be ensured by the MSI during the operations and maintenance period. These requirements shall be strictly imposed, and a third-party audit/ certification agency shall be deployed for certifying the performance of the MSI against the target performance metrics as outlined in the tables below.

18.2. SLA Management

i. The MSI shall provide proper plan, resources, and escalation procedure to NFAI to report problem case or support request during the warranty and Application Maintenance and Support periods.

ii. The MSI shall act as a single point of contact and follow-through with the principals of any third-party providers until the successful resolution of the case.

iii. The support hours for the website shall be:

Mondays to Friday 9.30am to 6.30pm

(For Saturday, Sunday, and Public Holidays at least One Technical resource must be available to handle issues)

iv. The MSI's key personnel shall always be contactable via phone.

v. The MSI's key personnel shall be on-site to handle severity level 1 problems. As a standard practice it is required to the MSI to provide a resolution Hierarchy and therefore an Escalation matrix to department for L1, L2 & L3 support with proper email ID and Contact number to be provided. However wherever required, the MSI senior technical/management will be required to visit NFAI Pune Phase I or Phase II offices for resolving critical issues.

vi. Upon notification of the problem, the MSI's personnel must respond within the required time specified in this tender during the support hours of the systems.

vii. The definition of the Priority level is as follows:

Priority Level	Description	Phone/Email Response Time 1	Resolution Time
P1	Causes severe loss of service. Affect the business operation continuity or unable to process critical functions	30 Mins	Within Two (2) hours on report of problem
P2	Causes minor loss of service. Affect a particular work area, but can continue to use for the other work areas using temporary	2 hours	Within one (1) working day on report of problem
P3	Causes no loss of service. The impact is an inconvenience, which may require a workaround to restore the functionality.	4 hours	Within three (3) working days on report of problem

18.3. SLA measurement and monitoring for equipment

The users of the system shall report the identified bug / problem/ non-functional component to the successful MSI through telephone / email / letter / verbally/ SLA monitoring tool. For SLA monitoring and Bug tracking MSI is encouraged to opt for vendor agnostic and open-source application for example Trac, Mantis Bug Tracker etc. The Cost associated with sourcing of the SLA monitoring tool and Bug tracking tool shall be the sole responsibility of the MSI. Resolution

time expected for various IT Components is given in the table below. Penalty shall be considered for the official working hours only (i.e., 9:30am to 6.30 pm). MSI need to either fully repair or replace the component by temporary substitute (of equivalent configuration) and make it functional (from the entire system perspective) within the expected resolution time. In case of temporary substitute, the original component needs to be replaced within 7 days else the penalty amount shall be considered. In case of major, damage, MSI needs to replace the component with the brand-new component of same or better specification, configuration, and capacity. The following table defines the SLA requirements for all project components as per the services:
The total outage minutes shall exclude all planned maintenance activities.

18.4. Implementation SLAs

18.4.i. **Parameters:** The SLA parameters for the implementation stage would be directly related to the delivery timelines of the deliverables as mentioned in the Timelines, Deliverables and Payment Schedule. This would consist of the entire commercial bid and the applications system with successful UAT of the same.

18.4.ii. **Period:** These SLAs would be applicable until NFAI Signoffs. The deliverables would be measured at every payment milestone as mentioned in the matrix (Refer Chapter 5)

Penalty Value: For delay of every week in completion & submission of the deliverable penalty shall be levied as below.

Delay (Weeks)	Penalty % on the respective Payment milestone value
1	0.5%
2	1%
3	1.5%

d. **Capping:** The upper limit of penalty would be capped at 5% of the Capital Expenditure . In case the successful MSI reaches the upper limit of penalty at any point of time during implementation phase, NFAI reserves the right to invoke the termination clause.

e. Delay of every week would also account in increase of additional 2 weeks in the maintenance period which will be over and above the maintenance period of 5 years. This duration would be accounted without incurring any charges to NFAI.

18.5. SLA for CSP (Cloud Service Provider)

The key service level objectives that relate to the cloud services and the related aspects are indicated below:

a) The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of NFAI, then NFAI will have the right to take appropriate disciplinary actions including termination of the contract.

b) The full set of service level reports should be available to NFAI on a quarterly basis

or based on the project requirements.

c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The CSP/MSI shall make available the Monitoring tools for measuring and monitoring the SLAs. The CSP may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every quarter which is to be shared with NFAI on a quarterly basis. NFAI shall have full access to the Monitoring Tools/portal and any other tools / solutions deployed for SLA measurement and monitoring) to extract data as required during the project.

d) The measurement methodology / criteria / logic will be reviewed by NFAI.

e) In case of default on any of the service level metric, the CSP shall submit performance improvement plan along with the root cause analysis for NFAI approval.

f) In case these service levels cannot be achieved at service levels defined in the agreement, NFAI shall invoke the performance related penalties. Payments to the MSI will be linked to the compliance with the SLA metrics laid down in the agreement.

S No	Service Level Objective	Measurement Methodology /	Target	Penalty
1	Availability of all provisioned Services which are provided by CSP including VM, Storage, DB, API gateways security services and any other critical services	Availability (as per the definition in the SLA) will be measured for each of the services over all the user types as defined in the RFP and NFAI users irrespective of service	Availability for each of the services over all the Portals and APIs (where applicable) >= 99.9%	Default on any one or more of the services will attract penalty as indicated below.
				<99.9% and >= 99.5% (1% of the Periodic Payment)
				<99.5% (2% of the Periodic Payment)
2	Availability of the links Internet and MPLS	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud to access the portal or admin services	Availability for each of the links:	Default on any one or more of the provisioned links will attract penalty as indicated below.
			>= 99.5%	<99.5% & >=99.0% (1% of the periodic Payment)
				< 99.0% (2% of the periodic Payment)
3	Availability of certification of compliance to the Empanelment of MeitY requirements		30 working days from the end of the Empanelment of MeitY	1% of periodic Payment
4	Response Time			<95% & >=90%

		Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15 minutes	(1% of the periodic Payment)
				< 90 (2% of the periodic Payment)
5	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1,	<98% & >=90%
			98% of the incidents Shall be resolved within 2 Hours of the reporting	(1% of the periodic Payment)
				< 90% (2% of the periodic Payment)
6	Time to Resolve - Severity 2	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity	<95% & >=90%
			2 within 6 hours of Incident reporting	(1% of the periodic Payment)
				< 90% & (2% of the periodic Payment)
	Security breach including Data Theft/Loss/Corruption/ unauthorized access	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For any security incident detected, penalty will be INR 1 Lakhs for each such incident.
7				This penalty is applicable per incident.
8	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time	10 working days from the end of the quarter	10 working days from the end of the quarter	1% of periodic Payment
9	Availability of Root Cause Analysis (RCA) ports for Severity 1 & 2		Average within 10 Working days	2% of periodic Payment
10	Setup of Cloud Environment	36 weeks from PO/LOA	No Delay	0.5% of one-time implementation cost per week delay

Note:

- Periodic Payment means Quarterly Payment for the associated service.
- Days: All Working and Non-working days (365 days in a calendar year)
- 24*7 means three shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days.
- Severity Levels: Below severity definition, provide indicative scenarios for defining

Incident's severity. However, NFAI will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and Compliance impacts.

Severity Level	Description	Examples
Severity 1	Production Environment is down, or critical malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention.	Non-availability of VM, Storage, API gateway, DB, Internet link and application containers and all security services.
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities, as essential functions and critical programs are partially available, the environment is usable but severely limited.	Intermittent network connectivity, UAT and SIT environment.

18.6. Penalty on non-adherence to SLAs for NFAI Website

- Any violation in meeting the SLA requirements for incident or resolving bug during warranty and maintenance period, NFAI shall impose a penalty of 0.2 % of total value of website maintenance for each day delay up to 5 % of website maintenance as maximum penalty. The penalty amount would be calculated and deducted on quarterly basis as may be decided by NFAI from time to time.

18.7. Post-Implementation SLAs

SLA Management and Monitoring Tool as specified in this RFP shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The third-party testing and audit of the system shall put sufficient emphasis on ensuring the capability of SLA Management and Monitoring Tool to capture SLA compliance correctly and as specified in this RFP. The selected MSI must deploy SLA Management and Monitoring tool and provide for capturing the required data for SLA report generation in automated way. This tool should generate the SLA Management and Monitoring report at the end of every month and every quarter which is to be shared with NFAI. NFAI will audit the tool and the scripts on a regular basis.

Where required, some of the Service Levels will be assessed through audits or reports e.g., utilization reports, measurements reports, etc., as appropriate to be provided by the MSI on a quarterly basis, in the formats as required by NFAI.

S. No	Parameter	Measurement of SLAs
1.	Infrastructure Related SLAs	SLA Management and Monitoring Tool
2.	Application related SLAs	SLA Management and Monitoring Tool

It may be noted that the MSI has to provision for the required tools to measure the SLA parameters. NFAI reserves the right to appoint Third Party for the audits. Audits will normally be done on regular basis or as required by NFAI and will be performed by NFAI or NFAI appointed third party agencies. MSI shall make provision when requisite permission is given to the Third-Party Agency for carrying out the audit process on regular basis.

18.7.1. Violations and Associated Penalties

The framework for Penalties, as a result of not meeting the Service Level Agreements Targets is as follows:

18.7.1.1. A quarterly performance evaluation will be conducted using the Quarterly reporting periods of that period

18.7.1.2. The performance will be measured for each of the defined service level metric against the minimum/ target service level requirements and the violations will be calculated accordingly.

18.7.1.3. The number of violations in the reporting period for each level of severity will be totaled and used for the calculation of Penalties.

18.7.1.4. Penalties applicable for each of the high severity (H) violations are one (1) % of respective Quarterly payment to the MSI.

18.7.1.5. Penalties applicable for each of the medium severity (M) violations is half percentage (0.5%) of respective Quarterly payment to the MSI.

18.7.1.6. Penalties applicable for each of the low severity (L) violations are Quarter percentage (0.25%) of respective Quarterly payment to the MSI.

18.7.1.7. Penalties applicable for not meeting a high (H) severity performance target in two consecutive Quarters on same criteria shall result in additional deduction of 3% of the respective Quarterly payment to the MSI. Penalty shall be applicable separately for each such high critical activity.

18.7.1.8. Penalties applicable for not meeting a medium (M) severity performance target in two consecutive Quarterly periods on same criteria shall result in additional deduction of 2% of the respective Quarterly payment to the MSI. Penalty shall be applicable separately for each such medium critical activity.

18.7.1.9. Penalties applicable for not meeting a low (L) severity performance target in two consecutive Quarterly periods on same criteria shall result in additional deduction of 1% of the respective Quarterly payment to the MSI. Penalty shall be applicable separately for each such low critical activity.

18.7.1.10. It is to be noted that if the overall penalty applicable for any of the review period during the contract exceeds 25% of the quarterly payment or if the overall penalty applicable for any of the successive Quarterly periods during the contract is above 15%; then NFAI shall have the right to encase the Performance Bank Guarantee or terminate the contract or both.

18.7.2. Operations and Maintenance Systems

18.7.2.1. Production Application

The failure or disruption of Live (in production) Application has a direct impact on the NFAI's ability to service its user units, ability to perform critical NFAI's functions or a direct impact on the organization. This includes but not limited to: -

i. Storage, Compute and Data hosted in cloud and DR
ii. Web, Application, Database, and Backup Servers
iii. Cloud, DR network infrastructure
iv. Cloud, DR security infrastructure
v. Connectivity and Availability of hosted Solution

The below tables give details on the Service Levels the MSI should maintain. These service levels will be monitored on a monthly basis and measured on a quarterly basis.

18.7.3. Service Availability

<table>
<tr><th>Service Level Description</th><th>Severity of violation</th><th>Measurement</th></tr>
<tr><td>Composite Service Availability should be minimum 99.95%</td><td>High</td><td>
<table>
<tr><th>Availability over the Quarter</th><th>No. of Violations to be counted for calculation of penalty</th></tr>
<tr><td>< 99.95% & >= 99.5%</td><td>1</td></tr>
<tr><td>< 99.5% & >= 99%</td><td>2</td></tr>
<tr><td>< 99%</td><td>3 for every percentage drop or part thereof below 99%</td></tr>
</table>
Composite Service Availability means availability and performance of infrastructure and application services for proposed Solution.
</td></tr>
</table>

18.7.4. Application Performance

a. The MSI is expected to submit a quarterly report on the availability of NFAI Enterprise Solution (NES).

Application Performance

The below tables give details on the Service Levels the MSI should maintain.

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td>1</td><td>Average Application Response Time</td><td>Medium</td><td>Average Application Response Time during peak usage hours as measured at any of NFAI's location shall not exceed 3 seconds.

The list of critical business functions and peak usage hours will be identified by NFAI during the Detail Design phase.

This service level will be measured on a quarterly basis.

<table><tr><th>Average Application Response Time over the Quarter</th><th>No. of violations post which penalty clause will be invoked</th></tr><tr><td>> 3 sec & <= 5 sec</td><td>2</td></tr><tr><td>> 5 sec & <= 8 sec</td><td>4</td></tr><tr><td>> 8 sec</td><td>5 for every second increase or part thereof exceeding 8 seconds</td></tr></table></td></tr>
<tr><td>2</td><td>Maximum Time for NES Home Page opening</td><td>Low</td><td>Maximum Time for NES Home Page opening during peak usage as measured at any of NFAI's location shall not exceed 2 seconds.

This service level will be measured on a quarterly basis.

<table><tr><th>Maximum Time for Home Page opening over the Quarter</th><th>No. of violations post which penalty clause will be invoked</th></tr><tr><td>> 1.5 sec & <= 3.5 sec</td><td>2</td></tr><tr><td>> 3.5 sec & <= 5.5 sec</td><td>3</td></tr><tr><td>> 5.5 sec</td><td>2 for every second increase or part thereof exceeding 5.5 seconds</td></tr></table></td></tr>
<tr><td>3</td><td>Menu Page after User Login</td><td>Low</td><td>Menu Page after User Login opening during peak usage as measured at any of NFAI's location shall not exceed 2 seconds.

This service level will be measured on a quarterly basis.</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Menu Page after User Login opening over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 1.5 sec & <= 3.5 sec</td><td>2</td></tr>
<tr><td>> 3.5 sec & <= 5.5 sec</td><td>3</td></tr>
<tr><td>> 5.5 sec</td><td>2 for every second increase or part thereof exceeding 5.5 seconds</td></tr>
</table>
</td></tr>
<tr><td>4</td><td>Menu Navigation – To display the menu as per the defined user role and profile</td><td>Low</td><td>Menu Navigation – To display the menu as per the defined user role and profile opening during peak usage as measured at any of NFAI's location shall not exceed 2 seconds.
This service level will be measured on a quarterly basis.
<table>
<tr><th>Menu Navigation – To display the menu as per the defined user role and profile over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 1.5 sec & <= 3.5 sec</td><td>2</td></tr>
<tr><td>> 3.5 sec & <= 5.5 sec</td><td>3</td></tr>
<tr><td>> 5.5 sec</td><td>2 for every second increase or part thereof exceeding 5.5 seconds</td></tr>
</table>
</td></tr>
<tr><td>5</td><td>Screen Opening – To display the selected data entry screen from the menu chosen</td><td>Low</td><td>Screen Opening – To display the selected data entry screen from the menu chosen during peak usage as measured at any of NFAI's location shall not exceed 2 seconds.
This service level will be measured on a quarterly basis.
<table>
<tr><th>Screen Opening – To display the selected data entry screen from</th><th>No. of violations to be counted for calculation of penalty</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>the menu chosen over the Quarter</th><th></th></tr>
<tr><td>> 1.5 sec & <= 3.5 sec</td><td>2</td></tr>
<tr><td>> 3.5 sec & <= 5.5 sec</td><td>3</td></tr>
<tr><td>> 5.5 sec</td><td>2 for every second increase or part thereof exceeding 5.5 seconds</td></tr>
</table>
</td></tr>
<tr><td>6</td><td>Response time to commit a transaction
• Simple Complexity
• Medium Complexity
• High Complexity
(Complexity of the transaction to depend on the complexity of the business logic and stored procedures committed at the database level)</td><td>High</td><td>Response time to commit a transaction during peak usage as measured at any of NFAI's location shall not exceed 4 seconds for Simple transactions, 7 seconds for Medium complexity transactions and 10 seconds for High Complexity transactions.
This service level will be measured on a quarterly basis.
Penalty for Simple transaction SLA violation
<table>
<tr><th>Response time to commit a Simple transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 4 sec & <= 6 sec</td><td>2</td></tr>
<tr><td>> 6 sec & <= 8 sec</td><td>3</td></tr>
<tr><td>> 8 sec</td><td>4 for every second increase or part thereof exceeding 8 seconds</td></tr>
</table>
Penalty for Medium Complexity transaction SLA violation
<table>
<tr><th>Response time to commit a Medium Complexity transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 7 sec & <= 9 sec</td><td>2</td></tr>
<tr><td>> 9 sec & <= 11 sec</td><td>3</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>> 11 sec</td><td>4 for every second increase or part thereof exceeding 11 seconds</td></tr>
</table>

Penalty for High Complexity transaction SLA violation
<table>
<tr><th>Response time to commit a High Complexity transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 10 sec & <= 12 sec</td><td>3</td></tr>
<tr><td>> 12 sec & <= 14 sec</td><td>4</td></tr>
<tr><td>> 14 sec</td><td>5 for every second increase or part thereof exceeding 14 seconds</td></tr>
</table>
</td></tr>
<tr><td>7</td><td>Response time for Screen with Query Retrieval
• Simple Query
• Medium Complexity Query
• High Complexity Query

(Complexity of the query will depend on the</td><td>High</td><td>Response time for Screen with Query Retrieval during peak usage as measured at any of NFAI's location shall not exceed 4 seconds for Simple Query, 7 seconds for Medium Complexity Query and 10 seconds for High Complexity Query.
This service level will be measured on a quarterly basis.
Penalty for Simple Query SLA violation
<table>
<tr><th>Response time for Screen with Query Retrieval for a Simple Query over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 4 sec & <= 6 sec</td><td>2</td></tr>
<tr><td>> 6 sec & <= 8 sec</td><td>3</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td>business logic, size of tables in databases being searched, indexing of database and the way procedures are written to retrieve information)</td><td></td><td>
<table>
<tr><td>> 8 sec</td><td>4 for every second increase or part thereof exceeding 8 seconds</td></tr>
</table>
Penalty for Medium Complexity Query SLA violation
<table>
<tr><th>Response time for Screen with Query Retrieval for a Medium level transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 7 sec & <= 9 sec</td><td>2</td></tr>
<tr><td>> 9 sec & <= 11 sec</td><td>3</td></tr>
<tr><td>> 11 sec</td><td>4 for every second increase or part thereof exceeding 11 seconds</td></tr>
</table>
Penalty for High Complexity Query SLA violation
<table>
<tr><th>Response time for Screen with Query Retrieval for a Complex transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 10 sec & <= 12 sec</td><td>3</td></tr>
<tr><td>> 12 sec & <= 14 sec</td><td>4</td></tr>
<tr><td>> 14 sec</td><td>5 for every second increase or part thereof exceeding 14 seconds</td></tr>
</table>
</td></tr>
<tr><td>8</td><td>Reports Generation</td><td>Medium</td><td>Reports Generation Response Time during peak usage as measured at any of NFAI's location shall not exceed 4 seconds for Simple Query, 7 seconds for Medium</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td>Response Time
• Simple Query
• Medium Complexity Query
• High Complexity Query
(Time of the report generation will depend on the complexity of the query, no. of parameters fetched, and level of customization required to generate the report)</td><td></td><td>Complexity Query and 10 seconds for High Complexity Query.
This service level will be measured on a quarterly basis.
Penalty for Simple Query SLA violation
<table>
<tr><th>Report Generation Response time from a Simple Query over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 4 sec & <= 6 sec</td><td>2</td></tr>
<tr><td>> 6 sec & <= 8 sec</td><td>3</td></tr>
<tr><td>> 8 sec</td><td>4 for every second increase or part thereof exceeding 8 seconds</td></tr>
</table>
Penalty for Medium Complexity Query SLA violation
<table>
<tr><th>Report Generation Response time from a Medium Complexity Query over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 7 sec & <= 9 sec</td><td>2</td></tr>
<tr><td>> 9 sec & <= 11 sec</td><td>3</td></tr>
<tr><td>> 11 sec</td><td>4 for every second increase or part thereof exceeding 11 seconds</td></tr>
</table>
Penalty for High Complexity Query SLA violation
<table>
<tr><th>Report Generation Response time from a High Complexity Query over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
</table></td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>> 10 sec & <= 12 sec</td><td>3</td></tr>
<tr><td>> 12 sec & <= 14 sec</td><td>4</td></tr>
<tr><td>> 14 sec</td><td>5 for every second increase or part thereof exceeding 14 seconds</td></tr>
</table>
</td></tr>
<tr><td>9</td><td>Maximum time for submission of forms/ data</td><td>High</td><td>Maximum time for submission of forms/ data during peak usage as measured at any of NFAI's location shall not exceed 4 seconds.
This service level will be measured on a quarterly basis.
Penalty for maximum time for submission of forms SLA violation
<table>
<tr><th>Response time to commit a Simple transaction over the Quarter</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>> 1.5 sec & <= 3.5 sec</td><td>2</td></tr>
<tr><td>> 3.5 sec & <= 5.5 sec</td><td>3</td></tr>
<tr><td>> 5.5 sec</td><td>2 for every second increase or part thereof exceeding 5.5 seconds</td></tr>
</table>
</td></tr>
<tr><td>10</td><td>Data Ingestion from Tape Library to Requestor (Film Festivals/ Theatres/ etc.)</td><td>High</td><td>Considering on-demand request for film titles (DCP or equivalent formats) to be sent to film festivals/ theatres/ award ceremonies to be encoded and made available for transfer via physical or online medium
Penalty for Data Ingestion SLA violation
<table>
<tr><th>Media Ingestion from Tape Library to NMAM</th><th>No. of violations to be counted for</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th></th><th>calculation of penalty</th></tr>
<tr><td>Online copy available to transfer within 96 Hours</td><td>3</td></tr>
<tr><td>Physical copy available to transfer within 178 Hours</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>11</td><td>Data Ingestion from Tape Library to Requestor (Users other than Film Festivals, theatre etc.)</td><td>High</td><td>Considering on-demand request for film titles (HD or equivalent formats) to be sent to users to be encoded and made available for transfer via physical or online medium
Penalty for Data Ingestion SLA violation
<table>
<tr><th>Media Ingestion from Tape Library to NMAM</th><th>No. of violations to be counted for calculation of penalty</th></tr>
<tr><td>Online copy available to transfer within 48 Hours</td><td>3</td></tr>
<tr><td>Physical copy available to transfer within 96 Hours</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>12</td><td>Born Digital films' data Ingestion from Tape Library to Requestor (format other than HD)</td><td>High</td><td>Considering on-demand request for film titles (DCP or equivalent formats) to be sent to requestor to be made available for online viewing
Penalty for Data Ingestion SLA violation
<table>
<tr><th>Media Ingestion from Tape Library to NMAM</th><th>No. of violations post which penalty clause will be invoked</th></tr>
<tr><td>Online copy available to transfer beyond 96 Hours</td><td>3</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>Online copy available to transfer between 96 hours to 144 Hours</td><td>4</td></tr></table></td></tr>
<tr><td>13</td><td>Data Ingestion from Tape Library to NFAI MAM (NMAM) on premise</td><td>High</td><td>Considering 5 TB of usable Data in the LTO tapes, the system should be able to ingest similar volume of Data onto the storage.
Penalty for Data Ingestion SLA violation
<table><tr><th>Media Ingestion from Tape Library to NMAM</th><th>No. of violations to be counted for calculation of penalty</th></tr><tr><td>> 36 Hours & <= 48 Hours</td><td>3</td></tr><tr><td>> 48 Hours & <= 60 Hours</td><td>4</td></tr><tr><td>> 60 Hours</td><td>5 for every hour increase or part thereof exceeding 30 Hours</td></tr></table></td></tr>
</table>

18.7.5. Handholding Support: Application Support

18.7.5.1. Level 1 (L1) Defects: The failure to fix has an immediate impact on the NFAI's ability to service its user units, inability to perform critical NFAI office functions or a direct impact on the organization.

18.7.5.2. Level 2 (L2) Defects: The failure to fix has an impact on the NFAI's ability to service its user units/ that while not immediate, can cause service to degrade if not resolved within reasonable time frames.

18.7.5.3. Level 3 (L3) Defects: The failure to fix has no direct impact on the NFAI's ability to serve its user units or perform critical NFAI's office functions.

18.7.5.4. The severity of the individual defects will be mutually determined by the NFAI and MSI.

18.7.5.5. This service level will be monitored on a monthly basis.

18.7.5.6. The below tables give details on the Service Levels the MSI should maintain.

<table>
<tr><th>Service Level Description</th><th>Severity of Violation</th><th>Measurement</th></tr>
<tr><td>Application Support Performance</td><td>High</td><td>95% of the Level 1 defects shall be resolved within 4 business hours from the time of reporting full details. This service level will be monitored on a monthly basis.
<table>
<tr><th>Performance over the Quarter</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 95% &>= 90%</td><td>1</td></tr>
<tr><td>< 90% &>= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
</table></td></tr>
<tr><td>Application Support Performance</td><td>High</td><td>95% of the Level 2 defects shall be resolved within 72 hours from the time of reporting full details.
This service level will be monitored on a monthly basis.
<table>
<tr><th>Performance over the Quarter</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 95% &>= 90%</td><td>1</td></tr>
<tr><td>< 90% &>= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
</table></td></tr>
<tr><td>Application Support Performance</td><td>High</td><td>100% of the Level 3 defects shall be resolved within 120 hours from the time of reporting full details.
This service level will be monitored on a monthly basis.
<table>
<tr><th>Performance over the Quarter</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 100% &>= 90%</td><td>1</td></tr>
<tr><td>< 90% &>= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table></td></tr>
</table>

18.7.6. Penalties shall not be levied on the successful MSI in the following cases

18.7.6.1. The noncompliance to the SLA has been solely due to reasons beyond the control of the MSI.

18.7.6.2. There is a Force Majeure event affecting the SLA, which is beyond the control of the MSI.

18.7.7. SLA Management for Website

i. The MSI shall provide proper plan, resources, and escalation procedure to NFAI to report problem case or support request during the warranty and Application Maintenance and Support periods.

ii. The MSI shall act as a single point of contact and follow-through with the principals of any third-party providers until the successful resolution of the case.

iii. The support hours for the website shall be:

Mondays to Friday 9.30am to 6.30pm
(For Saturday, Sunday, and Public Holidays at least One Technical resource must be available to handle issues)

iv. The MSI's key personnel shall always be contactable via phone.

v. The MSI's key personnel shall be on-site to handle severity level 1 problems. As a standard practice it is required to the MSI to provide a resolution Hierarchy and therefore an Escalation matrix to department for L1, L2 & L3 support with proper email ID and Contact number to be provided. However wherever required, the MSI senior technical/management will be required to visit NFAI Pune Phase I or Phase II offices for resolving critical issues.

vi. Upon notification of the problem, the MSI's personnel must respond within the required time specified in this tender during the support hours of the systems.

vii. The definition of the Priority level is as follows:

Priority Level	Description	Phone/Email Response Time [1]	Resolution Time [2]
P1	Causes severe loss of service. Affect the business operation continuity or unable to process critical	30 Mins	Within Two (2) hours on report of problem
P2	Causes minor loss of service. Affect a particular work area, but can continue to use for the other work areas using temporary	2 hours	Within one (1) working day on report of problem

Priority Level	Description	Phone/Email Response Time [1]	Resolution Time [2]
P3	Causes no loss of service. The impact is an inconvenience, which may require a workaround to restore the functionality.	4 hours	Within three (3) working days on report of problem

18.7.8. Penalty on non-adherence to SLAs

- Any violation in meeting the SLA requirements for incident or resolving bug during warranty and maintenance period, NFAI shall impose a penalty of 0.2 % of total value of website maintenance for each day delay up to 5 % of website maintenance cost as maximum penalty.
- The penalty amount would be calculated and deducted on quarterly basis as may be decided by NFAI from time to time

18.8. SLA for Media Ingestion Room (MIR)

The key service level objectives that relate to the cloud services and the related aspects are indicated below:

a) The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of NFAI, then NFAI will have the right to take appropriate disciplinary actions including termination of the contract.
b) The full set of service level reports should be available to NFAI on a quarterly basis or based on the project requirements.
c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The MSI shall make available the Monitoring tools for measuring and monitoring the SLAs. The MSI may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every quarter which is to be shared with NFAI on a quarterly basis. NFAI shall have full access to the Monitoring Tools/portal and any other tools / solutions deployed for SLA measurement and monitoring) to extract data as required during the project.
d) The measurement methodology / criteria / logic will be reviewed by NFAI.

e) In case of default on any of the service level metric, MSI shall submit performance improvement plan along with the root cause analysis for NFAI approval.
f) In case these service levels cannot be achieved at service levels defined in the agreement, NFAI shall invoke the performance related penalties. Payments to the MSI will be linked to the compliance with the SLA metrics laid down in the agreement.

S No	Service Level Objective	Measurement Methodology /	Target	Penalty
1	Availability of all provisioned Services which are provided by Media Ingestion Room	Availability (as per the definition in the SLA) will be measured for each of the services over all the user types and NFAI users irrespective of service	Availability for each of the services over all the Portals and APIs (where applicable) >= 99.95%	Default on any one or more of the services will attract penalty as indicated below. <99.95% and >= 99.5% (3% of the Periodic Payment) <99.5% (5% of the Periodic Payment)
2	Availability of the links Internet and MPLS	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the MIR to access the relevant modules	Availability for each of the links: >= 99.95%	Default on any one or more of the provisioned links will attract penalty as indicated below. <99.95% & >=99.5% (3% of the periodic Payment) < 99.5% (5% of the periodic Payment)
4	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15 minutes	<95% & >=90% (3% of the periodic Payment) < 90 (5% of the periodic Payment)
5	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents Shall be resolved within 2 Hours of the reporting	<98% & >=90% (3% of the periodic Payment) < 90% (5% of the periodic Payment)

S No	Service Level Objective	Measurement Methodology /	Target	Penalty
6	Time to Resolve - Severity 2	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 6 hours of Incident reporting	<95% & >=90% (3% of the periodic Payment) < 90% & (5% of the periodic Payment)
7	Security breach including Data Theft/Loss/Corruption /unauthorized access	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For any security incident detected, penalty will be INR 5 Lakhs for each such incident. This penalty is applicable per incident.
8	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time	10 working days from the end of the quarter	10 working days from the end of the quarter	5% of periodic Payment
9	Availability of Root Cause Analysis (RCA) ports for Severity 1 & 2		Average within 10 Working days	5% of periodic Payment
10	Setup of Cloud Environment	36 weeks from PO/LOA	No Delay	5% of one-time implementation cost per week delay

Note:

- Periodic Payment means Quarterly Payment for the associated service.
- Days: All Working and Non-working days (365 days in a calendar year)
- For this section 24*7 means one shifts of 8 hours every day. This is applicable for all seven days of the week without any non-working days.
- Severity Levels: Below severity definition, provide indicative scenarios for defining Incident's severity. However, NFAI will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and Compliance impacts.

Severity Level	Description	Examples
Severity 1	Production Environment is down, or critical malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention.	Non-availability of Tape Library, Storage, Internet link and application containers and all security services.
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities, as essential functions and critical programs are partially available, the environment is usable but severely limited.	Intermittent network connectivity, UAT and SIT environment.

Chapter 3: Instruction to Bidders

1. Completeness of Response

1.1. Bidders are advised to study all instructions, forms, terms, requirements, and other information in the RFP documents carefully. Submission of bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

1.2. The response to this RFP should be full and complete in all respects. Failure to furnish all information required by the RFP document or submission of a proposal not substantially responsive to the RFP document in every respect will be at the bidder's risk and may result in rejection of its Proposal.

2. Proposal Preparation Costs

2.1. The Bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in the conduct of informative and other due diligence activities, participation in meetings / discussions / presentations, preparation of Proposal, providing any additional information required by NFAI to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the Bid process. NFAI will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

2.2. This RFP does not commit NFAI to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award or for preparing this Bid. All materials submitted by the Bidder would become the property of NFAI and may be returned completely at their sole discretion.

3. Signing of communication with NFAI

All communications to NFAI including this RFP and the Bid documents shall be signed on each page by the authorized representative of the bidder and Power of Attorney as prescribed in Chapter 7: Section 7.2 thereby authorizing the representative to sign the documents related to the bid

should be submitted along with the Bid response. All the pages in the bid response / any communication with NFAI shall be numbered, signed by authorized representative, and stamped.

4. Amendment of RFP Document

4.1. At any time prior to the last date for receipt of Bid response, NFAI may, for any reason, whether at their own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP document through an amendment. The amendment will be published on the NFAI website (www.nfai.gov.in) and it shall be the responsibility of the Bidders to be vigilant about the updates uploaded by NFAI on their website.

4.2. In order to accord a reasonable time to the prospective Bidders to take the amendment into account for preparing their Bids, NFAI may, at their discretion, extend the last date for the receipt of Bids. The Bidders are allowed to resubmit their Bid, if required, after such amendments (but within the last date and time for submission of the Bids). If NFAI deems it appropriate to revise any part of this RFP or to issue additional data to clarify any provision of this RFP, they may issue a supplement / amendment / corrigendum to this RFP. Any such corrigendum shall be deemed to be incorporated into the RFP by this reference.

5. NFAI's right to modify submission deadline

NFAI may, in exceptional circumstances and at their discretion, extend the deadline for submission of Proposals by issuing a corrigendum on the NFAI website (www.nfai.gov.in). In such a scenario, all rights and obligations of the project and the Bidders previously subject to the original deadline will thereafter be subject to the extended deadline.

6. NFAI's right to terminate the process

NFAI may terminate the RFP process at any time without assigning any reason whatsoever. NFAI makes no commitments, express or implied, that this process will result in a business transaction with anyone. This RFP does not constitute an offer by NFAI.

7. Preparation and Submission of Responses

7.1. Softcopy Submission (Online Submission)

The Bidders should send/ submit their responses to **it@nfaipune.gov.in** with required details as follows:

7.2.1. Response should have following password protected documents and should be submitted as per schedule mentioned under Chapter 1: Section 4) –

7.2.1.1. A zip file and Link of the Drive containing softcopies of EMD, tender fees, pre-qualification documents with relevant Annexures and supporting documents. (Note: As per the schedule mentioned under Chapter 3: Section 7.2 of RFP).

7.2.1.2. Another zip file or Link of the Drive shall contain technical proposal with relevant annexures and supporting documents. (Chapter 3: Section 7.2)

7.2.1.3. A zip file or Link of the Drive consists of financial proposal with relevant annexures and supporting documents. (Note: As per the schedule mentioned under Chapter 3: Section 7.2 of RFP).

7.2.2. The three Folders/ Links should be in a single mail body.

7.2.3. A confirmation mail shall be sent to the bidders from NFAI (it@nfaipune.gov.in) intimating them on the receipt of the same.

7.2.4. Naming Convention:

7.2.4.1. Naming convention and format of the softcopies for Proposals will be as mentioned below:

#	Particulars	File Format	Password Protected (Yes/No)	Time for sharing the Password
1.	EMD and Tender fees_<<Prime bidder Name>>	Pdf	Yes	Post receiving an intimation from NFAI
2.	Pre-Qualification__<<Prime bidder Name>>	Pdf	Yes	Post receiving an intimation from NFAI
3.	Technical Proposal__<<Prime bidder Name>>	Pdf	Yes	Post receiving an intimation from NFAI

#	Particulars	File Format	Password Protected (Yes/No)	Time for sharing the Password
4.	Financial Proposal__<<Prime bidder Name>>	Pdf	Yes	During opening of financial proposals, post receiving an intimation from NFAI

7.2.4.2. All the above-mentioned files will be put in three folders. The bidder shall create three separate zip files of the folders. The said zip file shall be sent to NFAI. The naming convention to be followed for the zip file will be **"Proposal for Selection of MSI for NFAI's Enterprise Solution under NFHM by <Name of Prime bidder>".**

7.2.4.3. The bidder is required to share the password of document #1, #2 and #3 post receiving a confirmation mail from NFAI.

7.2.4.4. The password for document #4 shall be shared by the bidder at the time of opening of the respective financial proposals only. (Note: An intimation/ request mail for the same will be shared by NFAI in this regard)

7.2.5. No Deviation Bid:

7.2.5.1. It is required that all the Bids submitted in response to this RFP should be unconditional in all respects, failing which NFAI reserves the right to reject the Bid. The envelope should indicate the complete address and contact details of the Bidder to enable the return of the unopened bids in case it is declared "late".

7.2.5.2. The correspondence for any technical queries pertaining to this RFP and submission of Bid response must be made at the following address:

Officer on Special Duty, NFHM
National Film Archive of India,
Law College Road, Pune – 411 004.

8. Authentication of Bid

8.1. Authorized person of the bidder who signs the bid shall obtain the authority letter from the bidder, which shall be submitted with the Bid. All pages of the bid and its annexures, etc. shall be signed and stamped by the person or persons signing the bid. In case of consortium, only the person from Prime Bidder is authorized to sign the bid documents and no other person is permitted.

8.2. Power of Attorney executed by the Bidder in favor of the duly authorized representative, certifying him as an authorized signatory for the purpose of this bid.

9. Language of Bids

This bid should be submitted in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the bidder and summited with the bid, and English translation shall be validated at NFAI's discretion.

10. Patent Claim

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, or industrial design rights arising from the use of the Goods or any part thereof, the MSI shall expeditiously extinguish such claim. If the MSI fails to comply and NFAI is required to pay compensation to a third party resulting from such infringement, the MSI shall be responsible for such compensation, including all expenses, court costs and lawyer fees. NFAI shall give notice to the successful MSI of any such claim and recover it from the MSI if required or may ask MSI to settle such matter with due p1ayment necessary towards the same.

11. Late Proposal and Proposal Validity Period

Bids received after the scheduled time will not be accepted by the NFAI under any circumstances. NFAI will not be responsible for any delay due to postal service or any other means. The proposal validity period shall be for a period of 180 days from the proposal due date or any extensions thereof as mentioned in Chapter 1: Section 4 of this RFP.

12. Modification and Withdrawal of Proposals

Bids once submitted will be treated, as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids.

13. Non-conforming Proposals

A Proposal may be construed as a non-conforming proposal and ineligible for consideration:

13.1. If it does not comply with the requirements of this RFP

13.2. If the Proposal does not follow the format requested in this RFP or does not appear to address the particular requirement(s) of the NFAI.

14. Acknowledgement of Understanding of Terms

By submitting a Proposal, each Bidder shall be deemed to acknowledge that he has carefully read all sections of this RFP, including all forms, schedules, annexure, corrigendum, and addendums (if any) hereto, and has fully informed itself as to all existing conditions and limitations.

15. Bid Opening

15.1. Envelope A containing "Pre-qualification documents" shall be opened initially in the presence of Bidder and if the EMD and Tender Fee are as per the criteria then Envelope B of the qualified Bidder only shall be opened.

15.2. Envelope B containing the Technical Proposal shall be opened in the presence of the Bidder/ representatives of Bidder who choose to attend, at the address, date and time specified in the RFP.

15.3. Envelope C containing the Financial Proposal will remain unopened and will be held in custody of NFAI until the time of opening of the Financial Proposals.

15.4. At the end of the evaluation of the Technical Proposals, NFAI shall invite Bidder who have qualified for the opening of the Financial Proposals. The date, time, and location of the opening of Financial Proposals will be informed by NFAI separately and individually to qualified Bidder.

16. Letter of Award (LOA)

Prior to the expiration of the period of bid validity, NFAI will notify the successful bidder in writing or by fax or email, to be confirmed in writing by letter, that its bid has been accepted. LoA will constitute the formation of the contract. Upon the MSI's furnishings of Performance Band Guarantee, NFAI will promptly notify each unsuccessful bidder

17. Signing of Contract

After NFAI notifies the successful bidder that its Proposal has been accepted, NFAI shall enter into a Contract with the successful bidder, incorporating all clauses, Pre-Bid clarifications, Corrigendum(s), the Proposal of the Bidder, and any Government rules and GFR provisions. The Draft Legal Agreement is provided as a separate document as a template in Chapter 7: Section 7.15 and the same shall be signed with the successful bidder. The Legal Agreement is a draft and NFAI may finalize the same after legal consultations, and for the benefit of the project, and it shall be binding on the successful Bidder.

18. Failure to agree with the Terms & Conditions of the RFP / Contract

18.1. Failure of the MSI to agree with the Draft/after legal consultations the Legal Agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the Award, in which event NFAI may award the Contract to the next best value Bidder or call for new proposals from the interested bidders.

18.2. In such a case, NFAI shall invoke the EMD and the Performance Bank Guarantee of the MSI.

19. NFAI's Right to Accept any Bid OR to Reject any or All Bids

NFAI reserves the right to accept or reject any Bid, and to annul the bidding process and reject any or all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for NFAI's action.

20. Confidential Information

20.1. NFAI and the MSI shall keep confidential and shall not, without the written consent of the other party hereto, divulge to any third party any documents, data, or other information furnished directly or indirectly by the other party hereto in connection with the Contract, whether such information has been furnished prior to, during or following completion or termination of the Contract.

20.2. The MSI shall not use the documents, data, and other information received from NFAI for any purpose other than the services required for the performance of the Contract.

21. Change in Laws and Regulations

Unless otherwise specified in the Contract, if after the date of the Invitation for Bids, any law, regulation, ordinance, order, or bylaw having the force of law is enacted, promulgated, abrogated, or changed that subsequently affects the Delivery Date and/or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the MSI has thereby been affected in the performance of any of its obligations under the Contract.

22. Force Majeure

An event which is beyond the reasonable control of the bidder, is not foreseeable, is unavoidable and not brought about by or at the instance of the bidder claiming to be affected by such events and which has caused the non-performance or delay in performance, and which makes a bidder's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other extreme adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the bidder invoking Force Majeure to prevent), confiscation or any other action by Government agencies shall be termed as Force Majeure. Force Majeure shall not include:

22.1. Any event which is caused by the negligence or intentional action of the Bidder / Consortium member or by such their sub agencies (if any) or agents or employees,

22.2. Any event which a Bidder / Consortium member could have taken into account at the time of the execution of the project and avoid or overcome in the carrying out of its obligations.

22.3. Shall not include insufficiency of funds or inability to make any payment to fulfill any of its obligations for execution of the work shall not be considered to be a breach of, or default insofar as such inability arises from an event of Force Majeure, provided that the Bidder / Consortium member affected by such an event has taken all reasonable precautions, due care, and reasonable alternative measures, all with the objective of carrying out the scope of work as mentioned in this RFP.

23. Bid Security Declaration

a) Bidders shall submit, along with their Bids, Bid Security Declaration in favor of "Officer on Special Duty, NFAI", and should be valid for 6 months from the submission date of the Bidders Bids. (Refer Chapter 7: Section 7.5)

b) The Bid / Proposal submitted without Bid Security Declaration, as mentioned above, will be summarily rejected.

The clauses under Bid Security Declaration made by the bidder will be invoked if:

a) Bidder withdraws its bid before opening of the bids.

b) Bidder withdraws its bid after opening of the bids but before Notification of Award.

c) Selected Bidder withdraws its bid / Proposal before furnishing Performance Bank Guarantee.

d) Bidder violates any of the provisions of the RFP up to submission of Performance Bank Guarantee.

e) Selected Bidder fails to accept the order within five days from the date of receipt of the order. However, NFAI reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.

24. Performance Bank Guarantee

23.1. Within fifteen (15) working days from the date of issuance of LOA, the bidder shall at his own expense submit unconditional and irrevocable Performance Bank Guarantee (PBG) for an amount equivalent to 3% of contract value to NFAI.

23.2. The PBG shall be from a Nationalized Bank or a Scheduled Commercial Bank in the format prescribed in Chapter 7: Section 7.6 payable on demand, for the due performance and fulfilment of the contract by the bidder.

23.3. All charges whatsoever such as premium; commission etc. with respect to the PBG shall be borne by the bidder.

23.4. The PBG shall be valid till satisfactory completion of Post Implementation Support. The PBG may be discharged/returned by NFAI upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable on the PBG. The PBG shall hold good till 180 days after completion of the Contract Period.

23.5. In case the project is delayed beyond the project schedule as mentioned in the RFP, the PBG shall be accordingly extended by the bidder till completion of scope of work as mentioned in RFP.

23.6. In the event of the Bidder being unable to service the contract for whatever reason NFAI would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of NFAI under the contract in the matter, the proceeds of the PBG shall be payable to NFAI as compensation for any loss resulting from the bidder's failure to complete its obligations under the Contract. NFAI shall notify the Bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the Bidder is in default.

23.7. NFAI shall also be entitled to make recoveries from the bidder's bills, PBG, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction, or misstatement.

23.8. In addition to the PBG, the Successful Bidder shall submit a valid Bank Guarantee of the 110% of the advance payment made by NFAI. This Bank Guarantee shall be valid till the work under the advance is successfully completed.

On satisfactory performance and completion of the order in all respects and duly certified to this effect by NFAI, Contract Completion Certificate shall be issued and the PBG would be returned to the bidder.

Chapter 4: Evaluation Process

1. Evaluation Process

1.1. NFAI will constitute a Bid Evaluation Committee (BEC) to evaluate the responses of the bidders.

1.2. The BEC constituted by the NFAI shall evaluate the responses to the RFP (Envelope A, Envelope B and Envelope C) and all supporting documents / documentary evidence. Inability to submit requisite supporting documents / documentary evidence, may lead to rejection.

1.3. The decision of the Bid Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Committee.

1.4. The Bid Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their proposals. The Bidder shall submit requisite supporting documents/ certificates on the credentials. The BEC may visit prime bidder or any of its consortium member's client site to validate the credentials/ citations claimed by the Bidder.

1.5. The Bid Evaluation Committee reserves the right to reject any or all proposals

1.6. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.

1.7. The BEC would submit its decision to the competent authority whose decision would be final and binding upon the bidders.

2. Prequalification Criteria

2.1. Prequalification Evaluation Parameters

#	Eligibility Criteria	Document Proof
2.1.1.	The bidder or in case of a consortium, all the members of the consortium, must be incorporated / registered in India, under the Companies Act 1956/2013 or an LLP registered under the LLP Act 2008 or The Partnership Act 1932 Note: The consortium cannot be of more than 3 members (including Prime Bidder) All members of the consortium shall be jointly and severally liable for execution of the work	• Copy of Certificate of Incorporation/ Partnership Deed or equivalent, A duly notarized/ registered Joint Bidding Agreement/ Consortium Agreement) signed between Prime Bidder and all the consortium members. • Power of Attorney as per Chapter 6: Section 7 shall be submitted in case of a Consortium • The MoU should clearly mention detailed roles and responsibilities of the Prime Bidder and its Consortium members. .
2.1.2.	The bidder or in case of a consortium, **Prime Bidder** of the consortium should have completed at least One (1) project of an order value not less than INR 10 Cr. in any of the below mentioned activities within the last Five (5) years as on the last date of bid submission: i. Development and maintenance of an Enterprise software Solution(like Media Asset Management and Management of cloud-based archive)for Media &	• Work orders/ completion certificate/Go-Live certificate (as applicable) in the name of the bidder showing relevant work experience of past 5 years and above (Counting backwards from last date of bid submission) • Work order should clearly state complete start date of the project and should be signed by the issuing authority

	Entertainment Industry (Broadcasters/ Production Houses / OTT Players or Similar) ii. Deployment and maintenance of an Enterprise software Solution. iii. Work-related to deployment, commissioning of Tape library management or Hard Disk storage management for Media & Entertainment Industry (Broadcasters/ Production Houses / OTT Players)	
2.1.3.	The bidder or in case of a consortium, any member of the consortium should have completed at least One (1) project of an order value not less than INR 10 Cr. for Cloud hosting/ Cloud Management /Cloud Services within the last Five (5) years as on the last date of bid submission.	• Work orders/ completion certificate/Go-Live certificate (as applicable) in the name of the bidder showing relevant work experience of past 5 years and above (Counting backwards from last date of bid submission) • Work order should clearly state value of the project and complete start date of the project and should be signed by the issuing authority
2.1.4.	The bidder or in case of a consortium, the Prime Bidder should have an average annual turnover of INR 50 Cr. for the last three (3) financial years (2017-18, 2018-19, 2019-20)	• A certificate (on the letter head) from the practicing Chartered Accountant/Statutory Auditor duly signed & stamped and clearly mentioning the annual turnover details for a Single Entity and all members of the Consortium (in case of consortium) each year in the last three financial years (FY 2017-18, 2018-19, 2019-20)

		• Copy of the audited Profit and Loss Statement for Single Entity and all the members of the consortium including Prime Bidder (in case of consortium) for each of the last three financial years (FY 2017-18, 2018-19, 2019-20).
2.1.5.	The bidder or in case of a consortium, the all the members, should have positive net worth for last 3 years (2017-18, 2018-19, 2019-20).	• Net worth for last 3 years (2017-18, 2018-19, 2019-20) on CA letter head.
2.1.6.	The bidder or in case of a consortium, all the members of the consortium should not have been blacklisted by any State Govt. OR Central Govt. department OR organization in India OR abroad as on the last date of bid submission.	• Self-Certification by the single entity, prime bidder, and all members of the consortium on their respective letter head duly signed by the authorized signatory mentioning that the Bidder has not been blacklisted by any State Govt. or Central Govt. department and organization in India or abroad as on date of submission of this bid.
2.1.7.	Cloud Service Provider (CSP): 1. should be empaneled as CSP by the Ministry of Electronics & Information and Technology, Government of India as on the last date of bid submission. 2. The Data Centers should be owned and operated by the CSP. 3. The Cloud Service Provider (CSP) should be empaneled with the Ministry of Electronics & Information and Technology (MeiTY), Government of India for offering both DC & DR on its own (at least 2 data	• MeitY Empanelment Certificate in support of Sr 1 and 3 • Self-Declaration regarding Data center ownership and operation • c. Work order and self-declaration in support of Sr 4

	centers empaneled with MeiTY) to government bodies. 4. CSP should have deployed at least one project on GCC on cloud in last 3 years as on the last date bid submission.	

2.2. Evaluation of Prequalification Proposals

2.2.1. Bidders, whose EMD and Tender Document Fees are found in order, shall be considered for Pre-Qualification criteria evaluation.

2.2.2. Bidder shall be evaluated as per prequalification criteria mentioned at Chapter 4: Section 2.1. The bidders who fulfil all the prequalification criteria shall qualify for further technical evaluation.

3. Technical Evaluation Criteria

3.1. Technical Evaluation Parameters

#	Criteria	Scoring Criteria
3.1.1.	**Turnover** The bidder or in case of a consortium, the Prime Bidder should have an average annual turnover of INR 50 Cr. for the last three (3) financial years (2017-18, 2018-19, 2019-20)	**Max. Marks: 10** **• Average Turnover** **• 50 Cr. & <=75 Cr. – 5 Marks** **• 75 Cr. & <=100 Cr. – 7 Marks** **• >100 Cr. – 10 Marks**
3.1.2.	**No of Years in operations** The bidder or in case of the consortium, the Prime Bidder must be in business for at least 5 years as on the last date of bid submission. **Documents Required:** Incorporation certificate	**Max Marks: 10** **• Minimum 5 years – 5 marks** **• >5 years and <= 10 years – 7 marks** **• >10 years – 10 marks**
3.1.3.	**Cloud Service Provider experience** Experience in Cloud hosting /Cloud Services in the last 5 years as on the last date of bid submission. The value of each project shall not be less than INR 5 Crore.	**Max Marks: 15** **• 1 project - 5 marks** **• 2 – 3 projects - 10 marks** **• More than 3 projects - 15 marks**
3.1.4.	The bidder or in case of a consortium, any member of the consortium must have completed at least One (1) project that included any of the following components in its scope. The project shall have been completed in the last 5 years as on last date of bid submission: i. Content Network Delivery – design & deployment ii. Media Asset Management -– design & deployment iii. Over the Top (OTT) – design &	**Max Marks: 20** **• 1 Project - 10 marks** **• 2 Projects - 15 marks** **• More than 2 projects - 20 marks**

<table>
<tr><th>#</th><th>Criteria</th><th>Scoring Criteria</th></tr>
<tr><td></td><td>deployment
iv. Data Center – design & deployment
v. Cloud Hosting</td><td></td></tr>
<tr><td>3.1.5.</td><td>Manpower for O&M
Quality and adequacy of each of the following minimum proposed resources for the O&M phase, as per the details mentioned in the CVs of the resources:
• Project Manager
• Tape Library Expert
• Network Expert
• Post-production Expert
• Librarian/ Archivist (Cataloguing Expert)
• Website Developer</td><td>Max Marks: 20
<table>
<tr><th>Role</th><th>Work ex in years</th><th>Marks</th></tr>
<tr><td>Project Manager</td><td>10</td><td>5</td></tr>
<tr><td>Post-production Expert</td><td>7</td><td>3</td></tr>
<tr><td>Network Expert</td><td>7</td><td>5</td></tr>
<tr><td>Tape Library Expert</td><td>5</td><td>1</td></tr>
<tr><td>Librarian/ Archivist (Cataloguing Expert)</td><td>5</td><td>1</td></tr>
<tr><td>Website Developer</td><td>5</td><td>5</td></tr>
</table></td></tr>
</table>

#	Criteria	Scoring Criteria
3.1.6.	The bidder or in case of a consortium, any member of the consortium must have at least One (1) valid certificate of the following certifications as on the last date of bid submission: i. ISO 27001 ii. SEI CMMI level 3 or above certificate administered by ISACA The certificates must have been issued by the authorized certification agencies Note: The certificates must have been issued by the authorized certification agencies. NFAI may validate the authenticity of these certificates.	**Max Marks: 5** • ISO 27001 certificate- 3 marks • CMMI level 3 certificate - 1 mark • CMMI level 5 certificate - 2 marks
3.1.7.	Approach and Methodology: The Bidder's presentation would be evaluated on following criteria. •Understanding of the project scope and requirements – 25% weightage •Capability and Commitment level towards the project including the timelines with supporting examples/ case studies - 25% weightage •Overall solution proposed covering a case study, presentation/ demonstration – Here the bidder is expected to showcase the approach, work plan, implementation strategy for the Enterprise Platform, Media asset management, content delivery system, OTT, payment gateway and other modules specified in the RFP and timelines – 25% weightage •Quality Assessment / Quality Checks and adherence to the international standards – 25% weightage	**Max Marks: 20** Based on the Presentation

Note:

i. The bidders would need to submit documents as required in this RFP, to substantiate the evaluation criteria. The Bidder shall submit Work orders/ completion certificate/Go-Live certificate for projects submitted for TQ compliance.

ii. The Bid Evaluation Committee constituted by NFAI shall evaluate the technical bids based on proposal, documents submitted and presentations to arrive at the technical score.

iii. It is to be noted that the decision of the Bid Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence with the Bid Evaluation Committee regarding the evaluation process shall be entertained. The Bid Evaluation Committee reserves the right to reject any or all proposals on the basis of any deviations. Concealment or contradiction of facts would be held otherwise and liable for strict action. Any such incidence gives NFAI complete right to reject the claim of the bidder at any stage, even after the completion of tendering process, without even a formal notice.

iv. Each of the responses shall be evaluated to validate compliance of the bidders according to the criteria as per format and supporting documents mentioned against each clause

v. Bidder who meets the pre-qualification criteria shall be called for technical presentation (maximum duration of one hour) with respect to above technical evaluation criteria during Technical Bid Evaluation. Date, Time, and Venue for the Technical Presentation will be informed later to qualified bidders. NFAI reserves right to visit bidder's customer where such a similar project execution has taken place.

4. Evaluation of Technical Proposals

The evaluation of the Technical Proposals will be carried out in the following manner:

4.1. The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g., Detailed Project citations and completion certificates, client contact information for verification, and all others) as required for technical evaluation.

4.2. At any time during the Bid evaluation process, Bid Evaluation Committee may seek oral / written clarifications from the Bidders. The Committee may seek inputs from their professional and technical experts in the evaluation process.

4.3. NFAI reserves the right to do a reference check of the past experience stated by the Bidder. Any feedback received during the reference check shall be taken into account during the technical evaluation process.

5. Technical Evaluation Methodology

5.1. Each Technical Proposal shall be assigned a technical score out of a maximum of 100 points. (Refer Chapter 4: Section 4)

5.2. In order to qualify for the opening of financial proposal, the Bidder must get a **minimum overall technical score of 75 (Seventy-Five)** (Technically Qualified Bidders)

5.3. The Financial Proposals of Bidders who do not qualify technically shall be kept unopened.

5.4. NFAI reserves the right to accept or reject any or all bids without giving any reasons thereof.

5.5. NFAI shall inform the Technically Qualified Bidders about the date and venue of the opening of the financial proposals.

6. Financial Bid Evaluation

6.1. All the technically qualified bidders will be notified to participate in Financial Proposal opening process.

6.2. Financial Proposals for the technically qualified bidders will then be opened on the notified date and time and reviewed to determine whether the financial proposals are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at NFAI discretion.

6.3. Total Cost of Bid (TCB) shall be calculated based on the financial format given in Chapter 4: section 8 of the RFP. The bidder is required to provided commercial quote as per format Chapter 4: section 8 along-with cover letter as provided in Chapter 7: Section 7.12.

6.4. If there is a discrepancy between words and figures, the lower amount shall prevail. For any other calculation/ summation error etc. the bid may be rejected and EMD forfeited.

6.5. The cost indicated in the Financial Proposal shall be deemed as final and reflecting the total cost of services and should be stated in INR only. Omissions, if any, in costing of any item shall not entitle the Bidder to be compensated and the liability to fulfil its obligations as per the Terms of Reference within the total quoted price shall be that of the Bidder. The Bidder shall bear all taxes, duties, fees, levies, and other charges imposed under the Applicable Law as applicable.

7. Selection Methodology

The bids shall be evaluated using the Combined Quality Cum Cost Based system (CQCCBS) selection method as mentioned below:

7.1. The score secured based on evaluation of the Technical Bid as above shall be the Technical Score of the Bidder (X). Only those Bidders who score a **minimum of 75 marks** in the Technical Evaluation shall be considered for further evaluation.

7.2. The commercial quote shall be evaluated on the basis of total cost offered by the Bidder for the RFP. For any other calculation / summation error etc. the bid may be rejected.

7.3. Based on the Commercial Quote given by the Bidder, the Relative Commercial Score (Y), only for the Technically Qualified Bidders, will be calculated as below:

$$\text{'Y' of the qualifying Bidder} = \frac{\text{Lowest quoted offer of the qualifying Bidder}}{\text{Offer quoted by the respective qualifying Bidder}} \times 100$$

7.4. Final Composite Score for the Bidders shall be computed considering the Technical Score (X) and Relative Commercial Score (Y) and to be calculated as mentioned below:

Cs= (0.70 * X) + (0.30* Y)

Where,

Cs = Final Composite Bid Score

X = Total Technical score of the qualifying Bidder

Y = Total Relative Commercial Score of the Bidder

7.5. The Bidder shall be selected on the basis of **the Highest Composite Score (H1)**

7.6. In case two bidders get the same the Highest Composite Score (H1) then the bidder with the lowest quote will be selected.

7.7. In case the Bidder with the Highest Composite Score, rejects to accept/undertake the work, an offer at the sole discretion of NFAI shall be made to the Bidder with Second Highest Composite Score

7.8. The evaluation committee may visit the major facility of similar work being carried out by the selected MSI (India / Abroad / International Film Archive of Repute) before award of contract.

8. Commercial Bid Format

Financial Proposal should comprise of the following:

8.1. The bidder shall refer to the entire scope of this RFP for details on the functional and technical requirements and the benchmark specifications of the proposed solution for the items mentioned in the Financial Proposal and accordingly propose their respective cost.

8.2. NFAI also intends to utilize various rates obtained through this tender for requirements across various sections. Bidders are requested to factor this larger demand and give the best possible rates to NFAI.

8.3. The unit rates quoted for each individual line item shall be binding on the bidder for entire duration of the project.

8.4. Any bid which does not conform to the financial formats prescribed in the RFP will be disqualified.

8.5. Any conditional bid is liable for rejection.

8.6. Unless expressly indicated, bidder shall not include any technical information regarding the services in the financial proposal.

8.7. Prices shall be quoted entirely in Indian Rupees. All prices should be rounded off to the nearest Indian rupees (If the first decimal value is 5 (five) or above it should be rounded up and below 5 (five) should be rounded down). In cases of discrepancy between the prices quoted in words and in figures, lower of the two shall be considered.

8.8. No deviation in the contract price shall be made on account of any variations in unit rates or any cost component affecting the total cost in fulfilling the obligations under the contract. The contract price shall be the only payment payable to the successful bidder for completion of the contractual obligations by the successful bidder under the Contract, subject to the terms of payment specified in the contract. The price quoted would be excluding of GST. Prices quoted for the Solution shall be inclusive of license cost, installation, and commissioning. No extra payment on any account shall be admissible.

8.9. The prices, once offered, shall remain fixed and shall not be subject to escalation for any reason whatsoever within the period of project. A proposal submitted with an adjustable price quotation or conditional proposal may be treated as nonresponsive and rejected.

8.10. The amount stated in the Financial Proposal, adjusted in accordance with the above procedure, shall be considered as binding on the bidder for evaluation.

8.11. The bidder shall quote the total amount and shall upload the soft copy of breakup of cost as detailed in the Financial Proposal template provided under Chapter 4: Section 8, failing to which, NFAI may treat the bid as non-responsive and shall be rejected.

8.12. No Alternate Proposal: The bidder shall mention only one-unit price for each line item, only from single OEM/ Type for hardware, software, license, etc., to reach at consolidated cost as part of Financial Proposal. Any bids, which propose multiple options in terms of OEM/ Type and unit price for each line item shall be summarily rejected. For example, in case of licenses required, the bidder submitting two options of licenses for the same line item with different options for OEM/ Type or unit price shall be summarily rejected.

8.13. The Unit Rate as mentioned in the prescribed formats may be used for the purpose of 'Change Order or Additional Order' for respective items, if any. However, based on the market trends, NFAI retains the right to negotiate this rate for future requirement.

8.14. Bidder shall ensure that the future products supplied are of latest specifications as per the OEM roadmap.

8.15. Reduction in rates of any operation and maintenance or recurring charges should be adjusted as actuals, so that NFAI can reap benefits of reduction in rates.

8.16. For the purpose of evaluation of Financial Bids, NFAI shall make appropriate assumptions to arrive at a common bid price for all bidders. This however shall have no co-relation with the Contract value or actual payment to be made to the bidder.

8.17. NFAI will not be liable to pay any additional expenses or cost apart from the total cost mentioned in the Financial Proposal. Bidder needs to account for all Out-of-Pocket Expenses (OPE) due to Boarding, Lodging and other related items in the bid.

8.18. Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, lower of the two amounts will prevail.

8.19. Any misrepresentation or omission of any kind of applicable tax would be the sole responsibility of the bidder and NFAI would not be accountable or liable to pay for the same.

8.20. Table 1 refers to the Consolidated Cost Summary (excluding GST) which has two major line items specified as Capital Expenditure and Operating Expenditure.

The Qty mentioned for Table B.2 is for Tender evaluation and arriving at a tentative Project cost only. The payment for utilization of cloud services shall be made on actuals on a Quarterly basis subject to maximum cost as per the financial proposal.

Details for Financial Proposal

This table-1 should be consolidated to the "**Grand Total**" row from subsequent tables.

Note:

- **The bidder needs to provide for all costs required to run the solution for the entire duration of the contract.**
- **The bidder should not charge for any separate license fees to NFAI internal and external users for using the software solution.**
- **The bidder needs to account for all taxes in the Invoice submitted.**
- **All applicable taxes would be paid at actuals on the submitted Invoices.**
- **NFAI reserves the right to increase or decrease the line items and / or the quantity at the time of placing the work order.**

Table 1: Grand Total: Total Tender Value

Total Tender Value (Excluding of all Taxes)		
S. No	**Items**	**Total Price (Rs.)**
A	**B**	**C**
Capital Expenditure		
A.1	Media Ingestion Room	
A.2	Portal Development and Licenses	
A.3	Bandwidth	
A.4.	**Total Capital Expenditure**	
Operating Expenditure		
B.1	Training of NFAI staff	
B.2	Cloud Service Pricing	
B.3	O&M Manpower	
B.4	Web site and NES Operation & Maintenance for 5 Years	
B.5.	**Total Operating Expenditure**	
C.1	**Grand Total in figure (excluding GST) – (A.4.+ B.5.)**	
C.2.	**GST (as applicable)**	
C.3	**Grand Total in figure** (including GST) **– (C.1.+ C.2.)**	

Note:

i. The payment to the Bidder shall be made on the basis of actual work performed as per the quoted unit rates.

ii. It shall be mandatory for the respective Bidders to fill all the sections of the Commercial Bid format and failing to do so, the bids of the Bidder shall be liable for rejection.

iii. These rates shall be effective and valid throughout the contract period unless there is a drastic reduction in the market rates, in which case, the Bidder has to bring down his rates proportionately. The review of this would be carried out by NFAI once in every six months

iv. NFAI, at its sole discretion, may decide to delete/ remove any of the above-mentioned items or its quantity from the scope of the work any time during the course of bidding and/or execution of works.

v. The bidder needs to fill in all the sections for all tables (A.1, A.2, A.3., B.1, B.2, B.3 and B.4.) Provided herewith.

Sub-Table A.1: Media Ingestion Room (Exclusive of all Taxes)

Media Ingestion Room					
S. No	**Items**	**Qty**	**UoM**	**Unit Price (in INR)**	**Total Price (in INR)**
A	B	C	D	F	G = C x F
A 1.1	Ingest, Transcode, MAM Server (Server:16 Core 32GBRAM)	2.00	Nos		
A 1.2	Virtualization license	1.00	Nos		
A 1.3	DCP, Mezzanine and Editing Workstations (12-core Intel Xeon W processor, up to 4.4GHz or higher)	2.00	Nos		
A 1.4	QC Workstations (12-core Intel Xeon W processor, up to 4.4GHz or higher)	2.00	Nos		
A 1.5	UDP Acceleration Server / Appliance	5.00	per year		
A 1.6	Core Switch	2.00	Nos		
A 1.7	Access Switch	4.00	Nos		
A 1.8	Internet Router	2.00	Nos		
A 1.9	Next Generation Firewall	2.00	Nos		
A 1.10	Server Load Balancer	2.00	Nos		
A 1.11	Link Load Balancer	2.00	Nos		
A 1.12	Tape Library with three (3) Drives along with base frame with 500 slots, One Robotic Arm to handle up to 1000 Slots	1.00	Nos.		
A 1.13	LTO 7 cartridge	13,000.00@	Nos.		
A 1.14	LTO Cleaning Cartridge	6.00	Nos.		
A 1.15	SAN Switch	2.00	Nos.		

Media Ingestion Room

S. No	Items	Qty	UoM	Unit Price (in INR)	Total Price (in INR)
A	B	C	D	F	G = C x F
A 1.16	SAN Storage - Local Central Storage	1.00	Nos.		
A 1.17	Online UPS with 30 Mins battery backup	1.00			
A 1.18	Civil and Interiors for Media Ingest Room (Inclusive of furniture, civil work, electrical works, false ceiling, Fire etc.)	200.00	sqft		
A 1.19	Passive Network Components Including Patch Panel, LIU, OFC, Cat6 Cable, Patch Cords, Pipes, Installation & Labor Charges etc. (Bidders to give detailed breakup of the proposed components)	Lumpsum			
A 1.20	Post-Production Licenses	Lumpsum			
Total in figures (excluding GST)					**-**
GST (as applicable					
Total in figures (including GST)					
Total in words (excluding GST)					
Total in words (including GST)					

@- The quantity mentioned here is the max quantity that NFAI may require during the project duration and will be used for commercial evaluation purpose. The payment for this component will be made on the actual purchase basis and the unit rate shall be

considered for computation of payment. The unit rate shall also be considered for any purchase over and above the quantities mentioned above at the discretion of NFAI.

Sub-Table A.2: Portal Development and Licensing (Exclusive of all Taxes)

Portal Development & Licenses					
S. No	**Items**	**Qty**	**UoM**	**Unit Price (Rs.)**	**Total Price**
A	**B**	**C**	**D**	**F**	**G = C x F**
A.2.1	Design, Development, and Implementation and STQC of new NFAI website		lumpsum		
A 2.2	NES Portal Development		lumpsum		
A.2.3	MAM Licenses	1	Nos		
A.2.4	OTT Module	1	Nos		
A 2.5	Payment Gateway Module	1	Nos		
A.2.6	Email Gateway	1	Nos		
A.2.7	SMS Gateway	1	Nos		
A 2.8	Content Delivery Network	1	Nos		
A.2.9	Digital Asset Management	1	Nos		
A.2.10	Digital Rights Management	1	Nos		
A 2.11	Other Licenses (Please specify)				
Total in figures (excluding GST)					
GST (as applicable					
Total in figures (including GST)					
Total in words (excluding GST)					
Total in words (including GST)					

Sub-Table A.3: Bandwidth Costing (Exclusive of all Taxes)

Bandwidth Cost			
S. No	**Items**	**Qty**	**Total Price W/o GST(Rs.)**
A	**B**	**C**	**D**
A 3.1	Dedicated P2P Link to Cloud (100 Mbps)	Lump sum	
A 3.2	Dedicated ILL to Media Ingestion Room (100 Mbps)	Lump sum	
A 3.3	Dedicated fiber connection from Phase 2 to Phase 3 (6 Core)	Lump sum	
A 3.4	Dedicated P2P Link from Phase 2 to Phase 1 (50 Mbps)	Lump sum	
Total in figures (excluding GST) One Year)			
Total in figures (excluding GST) Five Year)			
GST (as applicable)			
Total in words (excluding GST) for Five years			
Total in words (including GST) for Five years			

Sub-Table B.1: Training of NFAI staff (Exclusive of all Taxes)

Training of NFAI Staff				
S. No	**Items**	**Qty**	**UoM**	**Total Price**
A	**B**	**C**	**D**	**E**
B 1.1	Training 1: post the period of two years after go-live of NES	1	lumpsum	

Training of NFAI Staff				
B 1.2	Training 2: refresher training at the end of fourth year after go-live of NES	1	lumpsum	
Total in figures (excluding GST)				
Total in figures (including GST)				
Total in words (excluding GST)				
Total in words (including GST)				

Sub-Table B.2: Cloud Pricing (Exclusive of all Taxes)

S. No	Items	Total Qty	UoM	Duration (in months)	Unit Rate (in INR)	Total Price (in INR)
A	B	C	D	E	F	G= C*E*F
B 2.1	Storage	500.00 #	*GB/month*	60		
B 2.2	DRM fees		monthly	60		
B 2.3	Forensic watermarking		yearly	5		

S. No	Items	Total Qty	UoM	Duration (in months)	Unit Rate (in INR)	Total Price (in INR)
A	B	C	D	E	F	G= C*E*F
B 2.4	One time transcoding of all the content	430,000.00#	Minutes			
B 2.5	Content Delivery Network	64.37 #	TB/ month	60		
Total in figures (excluding GST)						
Total in figures (including GST)						
Total in words (excluding GST)						
Total in words (including GST)						

The quantities mentioned here are for commercial evaluation purpose. The payment for these components will be made on the actual consumption basis and the unit rate shall be considered for computation of payment. The unit rate shall also be considered for any consumption over and above the quantities mentioned above at the discretion of NFAI.

Sub-Table B.3: Operation and Maintenance (Excluding GST)

Operations & Maintenance Manpower Cost					
S. No	**Items**	**Qty**	**UoM**		**Total Price (INR)**
A	**B**	**C**	**D**	**E**	**K=F+G+H+I+J**
A	**B**	**C**	**D**	**Duration (in months)**	**in INR**
B 3.1	Project Manager	1	Per month	60	
B 3.2	Post-Production Expert	1	Per month	60	
B 3.3	Network Expert	1	Per month	60	
B 3.4	Tape Library Expert	1	Per month	60	
B 3.5	Cataloguing Expert (Librarian/ Archivist)	1	Per month	60	
B 3.6	Website Developer	1	Per month	60	
Total in figures (excluding GST)					
Total in words (excluding GST)					

Sub-Table B.4: Website operations costing (Excluding GST)

Operations & Maintenance Manpower Cost for 5 years					
S. No	**Items**	**Qty (in years)**	**UoM**	**Unit Price (Rs.)**	**Total Price W/o GST(Rs.)**
A	**B**	**C**	**D**	**F**	**G = C x F**
B 4.1	Operations and Annual maintenance of NFAI website	5	Per Annum		
B.4.2	Operations and Annual maintenance of NFAI Enterprise Solution	5	Per Annum		
Total in figures (excluding GST)					
Total in figures (including GST)					
Total in words (excluding GST)					
Total in words (including GST)					

Chapter 5: Delivery Schedule & Payment Milestones

1. Payment Milestones

Sr. No	Milestone	Timeline	Payment in percentage terms
1	On team mobilization	T0+15 days	10% of Total Capital Expenditure
2	Finalization of Software Requirement Specification (SRS) and Design of Media Ingestion Room	T0+2 Months	10% of Total Capital Expenditure
3	On successful user acceptance test(UAT)	T0+5 Months	40% of Total Capital Expenditure
4	On successful Go Live	T0+ 6 Months	40% of Total Capital Expenditure
5	Operation and Maintenance (O&M Manpower, Cloud services, Web site and NES Operation & Maintenance for 5 Years)	5 Years post Go-Live	Cost for the OPEX in the financial proposal to be paid in 20 equal installments during the project period

Chapter 6: Technical Specifications

1. Technical Requirements

The bidders can propose appropriate industry standard products & solutions for the components required for implementation of the NFAI Media Ingestion Room (MIR). It is to be noted that NFAI may procure all /part of the Infrastructure Requirements/Services as specified in the RFP. It is not binding on the NFAI to procure all the infrastructure/services from the same organization and at the time of signing the contract.

1.1. Design Description

- Dedicated unshared bandwidth 100 Mbps Internet connectivity is proposed in the MIR
- The MIR located in Phase 2 should be capable of connecting with the new Phase 3 facility with a dedicated fiber (6 Core) connection, when the Phase 3 facility is operational.
- The MIR should be capable of connecting Phase 1 and Phase 3 facility with a minimum of 50 Mbps P2P connection.
- Intrusion Detection & prevention system should detect malicious traffic from Internet/extranet network and further protect the MIR environment.
- Firewalls would provide next layer of protection between the DMZs
- All the servers would be connected to high-capacity LAN Switch, which can process millions of packets within seconds, depending on the Users and Application and its contents.
- The MIR will provide Infrastructure Services such as storage Service, security services, internet bandwidth, etc.
- For Securing the MIR, the Intrusion prevention systems shall carryout state-full inspection and multiple layers of Firewalls shall manage the access control. At the same time more specific content level scanning products like Anti-Spam, network anti-virus gateways

should be provisioned at appropriate points to ensure content level scanning, blocking and access.

- In this secure infrastructure it has to be ensured that the security devices in the network such as Firewalls, Anti-Spam Filters, proxy servers, anti-virus gateways are in high-availability mode, and these devices should be even distributed to optimize performance.
- Another key consideration should be done for hosting the Legacy applications.

NOTE: ALL THE EQUIPMENT NEED TO BE BRAND NEW AND OF LATEST MAKE/MODEL (MANUFACTURED POST Jan 2020). ADDITIONALLY, THE SAME NEEDS TO BE PROCURED BY THE BIDDER AT THEIR OWN COST.

2. NFAI Media Ingestion Room (MIR) Architecture – Physical Infrastructure

2.1. Layout of the MIR

The entire MIR area will be logically divided in Zones Each of these zones Shall having different objective described further in this section. The respective area of each Zone would actually vary, primarily on the basis of number of applications and Size.

a. Zone A – Automatic Tape Library with the Robotic Arm along with , Server Racks, Storage racks and Networking component etc.
b. Zone B – Comprises of Workstations attached to the Media Ingestion Server
c. Zone C – Comprises of UPS & Electrical Room, Batteries Room etc.

A detailed description of key areas of MIR is given below:

2.1.1. Zone A – Automatic Tape Library, Compute and Network components

This area will contain Automatic Tape Library, Local Central Storage, Servers and all the required the networking components from routers, switches, Firewalls to passive components. The data communication component area will terminate LAN Connections and host a network monitoring station for LAN. All the MIR LAN connections will be provided through switches placed in this area.

This area will host the Security components. The security architecture will provide controlled access to the web and database servers from Internet and other networks. This would be multi-

layer architecture with two layers of firewall separating the Internet, web, and database/application and Intranet zones.

2.1.2. Zone B - Editing and QC Workstations Room

This room will have all the necessary arrangements for the Editing and Quality Check Workstations required to Ingest, Edit, and run quality checks for the content in the Local Central Storage as well as accessing the Automatic LTO Library

MIR shift operators taking care of daily operational activities of MIR will use this area. There will be one Media Ingestion Room (MIR) In charge per shift sitting in this area along with shift operators (one each for specific activities like backup, daily MIR administration / operations etc.)

2.1.3. Zone C - UPS and Electrical Room

This area shall house all the Un-Interrupted Power Supply Units, Main Power Distribution Units (PDU) and Sub Distribution Units to feed the components such as PAC, UPS, lighting, fixtures etc. It is recommended to install transformer based PDUs in the Media Ingestion Room.

It is also being proposed that the UPS and Electrical Room be located on the ground floor to avoid battery load to come on the building. However, the final decision in this regard shall be taken by NFAI in consultation with MSI.

2.1.4. Humidity, Ventilation and Air Conditioning Systems

The Media Ingestion Room should be precision environment controlled. The temperature inside Media Ingestion Room should be maintained at 12 degree centigrade with a precision of ± 1 degrees. The Precision Air Conditioning shall be provided for the Media Ingestion Room where the active equipment like Servers, storage & network components are housed. It is suggested to provide air supply typically through false flooring/celling.

2.1.5. Air Conditioning

Since Zone A & Zone B are critical areas, a separate air conditioning system (precision air conditioning) should be exclusively installed to maintain the required temperature for these Zones. The general requirements for the two zones are as specified below:

- Zone A – should be provided with precision air conditioning on a 24 x 7 x 365

days operating basis having n + 1 redundancy architecture requirements and having enough provision to scale it to next level as may be required in a later stage. The units should be able to switch the air conditioner on and off automatically and alternately for effective usage in pre-defined sequence. The units should be down-flow fashion, air-cooled conditioning system. Precision Air Conditioning systems specifically designed for stringent environmental Control with automatic monitoring and control of cooling, heating, humidification, dehumidification, and air filtration function should be installed.

- Zone B - Should be provided with split-type comfort air-cooled system

2.1.6. Ducting Requirements

It is Ideal for higher power system the gap between false floor and true floor should be used to deliver conditioned air to the desired space, the Floor Discharge System to eliminate the requirement of duct. This can be taken care as and when such system comes to MIR to such needs. However, proper ducting mechanisms should be ensured for the requirement of Air Conditioning.

2.1.7. Natural Convection

As the conditioned air is supplied through the grills with volume control dampers on the floor, the cold air-cools the component in a much faster and efficient manner as it does moves up, after extracting heat from the component. This follows the natural convection path of the air. The warm air should be sucked at the top by machine, air-conditioned and then supplied back to the room.

2.1.8. Air Distribution

The air is to be distributed evenly by providing grills with VCDs (Volume Control Dampers) in the floor tiles.

2.1.9. Flexibility

The system should give the flexibility of discharging air at wherever point required even if the furniture is relocated. Changing the grill/tiles carrying grills, at suitable location does this.

2.1.10. Rodent Repellant

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

- Configuration : Master console with necessary transducer
- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 50 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

2.1.11. False Ceiling

The top false ceiling would have 1' 6'' feet of space from the actual Room ceiling. This false ceiling will house AC ducting (if required) and cables of Electrical lighting, Firefighting, Rodent Control and CCTV.

2.1.12. UPS Requirements & Features

UPS System design concept is based on redundancy and availability with true online system. To support the dual bus system configuration three units of UPS should be installed. The Zone An area should have three parallel redundant UPS and other areas like NOC, BMS and Staging Area should have a separate UPS system. Dual redundant UPS systems will take care of following needs –

- Servers
- Access Control / Fire Detection, suppression / surveillance system

The solution should be automatic with power supply from the transformer as the primary source and automatic switchover to DG set as a secondary source for the data center. Earthing should be provided from the electrical room control panel to the Earthing pits.

It is recommended to have 2 UPS with 60 minutes battery back-up on each UPS for redundant purpose. The UPS system shall be provided with a capacity to accommodate the active components in the Media Ingestion Room for 60 Minutes. (number of racks may increase/ decrease as per MSI's solution) in an area of 200 sq. ft.

<u>UPS Modes of Operation</u>

- The UPS shall operate as an ONLINE reverse transfer system in the following modes:
  - Normal - The UPS inverter continuously supplies the critical AC load. The rectifier / charger derives power from AC Input source and supplies DC power to the Inverter while simultaneously load charging power reserve battery.
  - Emergency (Failure of AC Input) – Upon failure of AC Input power, the critical AC load will be supplied by the Inverter, which without any switching obtains power from the battery. There shall be no interruption in power to the critical load upon failure or restoration of the AC input source.
  - Recharge – Upon AC power restoration the rectifier / charger shall automatically restart and supply power to the inverter and start charging the batteries.
  - Bypass – A static transfer switch should be provided for performing reverse transfer of the load from the inverter to bypass source with no interruption in the power to the critical AC load. A manually operated maintenance bypass switch should be incorporated into UPS cabinet that will connect the load to AC power source bypassing the rectifier charger inverter and static transfer switch. The battery circuit breaker MCCB shall have O/L and U/V protection. The UPS shall have built in isolation transformer in order to isolate neutral of incoming supply from the load. The load has to be provided separate neutral generated by the secondary winding of output isolation transformer.
  - Paralleling Operations: The output of all the three UPS systems should be directly connected at the load distribution panel through individual circuit breakers (part of the distribution panel). The load at the output should be shared equally by all the UPS systems. The paralleling control mechanism should be available with individual UPS. There should not be any single point of failure which can lead to collapse of all the UPS systems.

2.1.13. Battery Requirements

Battery Bank should be designed to provide 30 minutes back up at full load for Media Ingestion Room equipment . Battery should be sealed and maintenance free type. The plates shall be designed for maximum durability during all service conditions including high rate of discharge and rapid fluctuation of load. The UPS Module should have the battery circuit breaker mounted near to the batteries. When this breaker is opened no battery voltage should be present in the

enclosure. The battery breaker should be automatically disconnected when the battery reaches to minimum discharge voltage level or when signaled by other control functions. Remote tripping of Battery circuit breaker facility shall be also incorporated. The batteries should be housed in suitable Racks. Battery installation shall be outside the MIR area to avoid fire hazard as recommended by NFPA guidelines.

2.1.14. Power Distribution

- Battery installation shall be outside the Zone A & Zone B area to avoid fire hazard as recommended by NFPA guidelines.
- For power transfer from normal to emergency, automatic power transfer switches (ATS) with bypass shall be used as per tier regulations. The ATS shall have overlapping neutral as stipulated by IEEE for electronic switching applications.
- Power cabling inside the MIR shall be of copper. The cables and conduits used inside the MIR shall be of FRLS quality.
- Signal referencing copper Earthing to be used using braided copper wire of 6 Gauge inside the MIR.

2.1.15. Electrical Work for Media Ingestion Room

The electrical cabling Work shall include the following:

- Main electrical panel in Media Ingestion Room (MIR)
- Power cabling
- UPS Distribution Board
- UPS point wiring
- Power Cabling for Utility component and Utility Points etc.
- Online UPS
- Separate Earth Pits for the component

The distribution of power from the UPS room to the following shall be considered:

- All proposed component for the production environment in the Media Ingestion Room
- Existing servers and another component
- UPS 2 Nos. each with static bypass arrangement

- Sub distribution panels for UPS
- Final Distribution shall be through Power Distributions Units (PDU)/MCB Distribution Boxes. Power in the racks and other components shall be provided with three sockets with power coming from separate UPS in each of these sockets.
- The bidder is required to maintain two electrical distribution paths (one normal & one alternate) for the cabling inside the server farm area in the proposed Media Ingestion Room (MIR)

Specifications for Electrical Cabling – Fire retardant cables of rated capacity exceeding the power requirement of fully blown configuration of the existing and proposed component to be used. For expansion needs suitable redundant power points to be provided at suitable locations. All materials used shall conform to IS standards as per industry practice.

- Bunching of Wires – Wires carrying current shall be so bunched in the conduit that the outgoing and return wires are drawn into the same conduit. Wires originating from two different phases shall not be run in the same conduit.
- Drawing of Conductors – The drawing Aluminum / Copper conductor wires shall be executed with due regards to the following precautions while drawing insulated wires into conduits. Care shall be taken to avoid scratches and kinks, which cause breakages.
- Joints – All joints shall be made at main switches, distribution boards, socket outlets, lighting outlets and switch boxes only. No joints shall be made inside conduits and junctions' boxes. Conductors shall be continuous from outlet to outlet.
- Mains & Sub-Mains – Mains & sub-mains wires were called for shall be of the rated capacity and approved make. Every main and sub-main shall be drawn into an independent adequate size conduit. Adequate size draw boxes shall be provided at convenient locations to facilitate easy drawing of the mains and sub-mains. An independent earth wire of proper rating shall be provided. The earth wires shall run along the entire length of the mains and sub-mains.
- Load Balancing – Balancing of circuits in three-phase installation shall be planned before the commencement of wiring.
- Color Code of the Conductors – Color code shall be maintained for the entire wiring installation, Red, Yellow, Blue for three phases and "OFF" circuit black for neutral and green for earth (or bare earth).

- Fixing of the Conduits – Conduit's junction boxes shall be kept in position and proper holdfasts shall be provided. Conduits shall be so arranged as to facilitate easy drawing of the wires through them. Adequate junction boxes of approved shape & size shall be provided. All conduits shall be installed so as to avoid stream and hot water pipes. After conduits, junction boxes, outlet boxes & switch boxes are installed in position their outlets shall be properly plugged so that water, mortar, insects, or any other foreign matter does not enter into conduit system. Conduits shall be laid in a neat and organize manner as directed and approved by the Information Technology Department Personnel or person on their behalf. Conductors shall be planned so as not to conflict with any other service pipelines / ducts.
- Protection – To minimize condensation or sweating inside the conductors all outlets of conduit system shall be adequately ventilated and approved by the proper competent authority. All screwed and socketed connections shall be adequately made fully watertight by use of proper jointing materials.
- Switch-Outlet Boxes and Junction Boxes – All boxes shall conform to all prevailing Indian Standards. The cover plates shall be of best quality Hylam sheets or ISI grade Urea Formaldehyde Thermosetting insulating material, which should be mechanically strong and fire retardant. Proper support shall be provided to the outer boxes to fix the cover plates of switches as required. Separate screwed earth terminals shall be provided inside the box for earthling purpose.
- Inspection Boxes – Rust proof inspection boxes of required size having smooth external and internal Finish shall be provided to permit periodical inspection and to facilitate removal and replacement of wires when required.

3. Technical Specifications – Physical Components

3.1. Infrastructure – Media Ingestion Room (MIR)

A. This part is related to the supply, installation & configuration of infrastructure components required to build and operate the Media Ingestion Room which will include server, storage, security devices and related system software. An indicative infrastructure is provided. However, MSI can recommend the IT infrastructure based on their solution approach & platform; complying with the baseline technical

requirements provided in this RFP. MSI has to design the infrastructure based on their proposed components required to be housed ensuring an integrated system capable of all the functional & architectural requirements mentioned in the RFP.

B. IT infrastructure is required to ingest data from Tape Library to the Enterprise solution hosted in cloud.

C. The infrastructure is required to support dedicated UDP File Acceleration for uploading content to the cloud

D. MSI will supply the infrastructure components based on BOQ submitted in the proposal.

E. The Media Ingestion Room will house the following active equipment:

i. Core Network Switch
ii. Network Access Switch
iii. Internet Router
iv. Next Generation Fire Wall
v. Tape Library with Robotic Arm
vi. SAN Switch
vii. Local Central Storage
viii. Ingestion Server
ix. Workstation

F. Activities for this part are as follows:

i. Infrastructure Requirement

MSI has to build infrastructure for Media Ingestion Room to support the proposed NES solution in terms of functionalities, availability as well as performance. MSI has to supply, install, commission, and maintain all the required civil infrastructure along with software, hardware, and accessories for the same. NFAI will provide space for building the Media Ingestion Room

ii. Infrastructure Components for Media Ingestion Room

Following are the broad categories of Infrastructure components and respective minimum functional and technical requirements:

A	Core Network Switch
S. No.	**Minimum Technical Specifications**
1	**Solution Requirement**
	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 inbuilt level of redundancy
2	**Hardware and Interface Requirement**
	Switch should have the 48 x 1/10G/25G fiber ports and should have 8 x 40/100G QSFP+ ports
	Switch should have 16GB DRAM and 16GB Flash/Storage
	Switch should support Configuration roll-back
	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.
	The switch should support 100,000 IPv4 routes and 100,000 IPv6 routes entries in the routing table including 48,000 multicast routes
	The switch should support hardware-based load sharing at wire speed using LACP and multi chassis ether channel/LAG
	The switch should have 32MB buffer
	Switch should support minimum 4 Tbps of switching capacity
3	**Layer2 Features**
	Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)
	Switch should support minimum 200,000 no. of MAC addresses
	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 32 number of ports per Link Aggregation Group
	Support for broadcast, multicast, and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
	Switch should support Ethernet Switch Identifier - Link aggregation groups (ESI-LAG) to enable one or more servers to multi-home to the Leaf Switches
4	**Layer3 Features**
	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
	Switch should support static and dynamic routing like Static, OSPF and BGP
	Switch should provide multicast traffic reachable using PIM-SM and SSM, BFD
	Should support a datacenter Fabric build on mature standards and protocols such as BGP EVPN/VXLAN to normalize datacenter and fabric operations. No proprietary solutions are to be deployed for fabric
	Should support dynamic load balancing in an EVPN-VXLAN network when a multihomed device can be reached through multiple virtual tunnel endpoints (VTEPs) that share a common Ethernet segment identifier (ESI)

A	Core Network Switch
	Switch should have following IPv4 & IPv6 routing enabled from day one - OSPF, BGP, EVPN-VXLAN, PBR, GRE, IS-IS, Q-in-Q, VRF & VRRP
	Switch should support following IPv4 & IPv6 routing with an additional license - MPLS, L2 & L3 VPN, L2 & L3 VXLAN Gateway
5	**Availability**
	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP
	Switch should support for BFD For Fast Failure Detection
6	**Quality of Service**
	Switch system should support 802.1P classification and marking of packet CoS, DSCP etc.
	Switch should support for different type of QoS features for ream time traffic differential treatment using WRED and SP Queuing
	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x/PFC (802.1Qbb)
7	**Security**
	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V4 and IP V6 and logging for fault finding and audit trail
	Switch should support control plane i.e., processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
	Switch should support for external database for AAA using TACACS+ / Radius
	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
8	**Manageability**
	Switch should support for embedded RMON/RMON-II for central NMS management and monitoring
	Switch should provide remote login for administration Telnet, SSHv2
	Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP V2 and V3
	Switch should support for basic administrative tools like Ping and traceroute
	Switch should support XML (NETCONF) based configuration
	Switch should support central time server synchronization using Network Time Protocol NTP

A	Core Network Switch
9	**IPv6 features**
	Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such as OSPFv3, BGP+ etc.
	Should support route redistribution between these protocols
10	**Safety and Compliances**
	Switch should be Common Criteria NDPP/NDcPP certified
11	**Warranty**
	Switch should be provided with hardware replacement warranty and ongoing software upgrades for all major and minor releases for a period of 5 years and AMC for additional 2 years

B	Network Access Switch
S. No.	**Minimum Technical Specifications**
1.	Minimum 24 x 10/100/1000 Base-T and 4 x 1/10G ports (with required transceiver modules)
2.	1 U Rack mountable and should provide stacking of minimum 8 switches with 80 Gbps of dedicated stacking/ equivalent bandwidth (All the stacking accessories should be included from day 1).
3.	The Switch should have 2GB DRAM and 2GB internal Flash
4.	128Gbps or higher Backplane capacity and minimum 95 Mpps of forwarding rate (excluding the stacking bandwidth and forwarding)
5.	Should support Non-blocking hardware architecture
6.	All interfaces should provide wire speed forwarding for both Fiber and copper modules
7.	Support for at least 2000 VLANs & 32k MAC address
8.	It should support IGMP snooping v1, v2 & v3
9.	It should have static IP routing from Day 1 and should be upgradable to support OSPF and PIM
10.	Switch should support 8 hardware queues per port
11.	Dynamic Host Configuration Protocol (DHCP) snooping
12.	Switch should support LLDP capabilities
13.	Should support IP Source Guard, DAI and IPv6 Security feature like IPv6 RA Guard and IPv6 Neighbor Discovery Inspection
14.	Should support Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3).
15.	Switch needs to have console port for administration & management
16.	Management using CLI, GUI using Web interface should be supported
17.	FTP/TFTP for upgrading the operating System
18.	Should support Energy Efficient Ethernet

B	Network Access Switch
19.	IEEE 802.1x support, IEEE 802.1D Spanning-Tree Protocol, IEEE 802.1p class-of-service (CoS) prioritization, IEEE 802.1Q VLAN, IEEE 802.3 10BASE-T specification, IEEE 802.3u 100BASE-TX
20.	Switch should support internal redundant power supply and Hot swappable fans
21.	Switch should be able to support management via CLI, Web interface
22.	SNMP v1, v2, v3
23.	Switch should be manageable through both IPv4 & IPv6.
24.	Switch should be UL-UL60950-1, FCC Part 15, VCCI Class A, EN 55022, EN 55024, EN 300386, CAN/CSA 22.2 No.60950-1, Reduction of Hazardous Substances (ROHS) certified
25.	Switch Should be Common Criteria NDPP/NDcPP certified

C	Internet Router
S. No	**Minimum Technical Specifications**
1.	**Architecture:**
	The appliance-based security platform shall be capable of providing firewall, IPS and VPN (IPSec) functionality simultaneously.
	The Router should support Advanced Threat Protection like malware and zero-day threats through cloud subscription or should integrate with on premise APT solution
	Should provide Stateful failover.
	Should have routing capacity of at least 550Kpps
	Should provide active/active and active/standby failover
	Should support Up to 256K Concurrent sessions
	Should provide 200 Mbps IPSec throughput
2.	**Memory -** Should have 4Gb RAM and 8Gb Flash
3.	**Support: -** IKEv1 and v2, IPSec VPN standards, 56-bit DES, 168-bit 3DES, 256-bit AES encryption
4.	**Authentication, Authorization and Accounting (AAA) support:** RADIUS or TACACS+
5.	**Support for:** Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256
6.	**Provides:**
	Rich dynamic NAT and PAT services
	Static NAT and PAT services
	Stateful and stateless and Zone-based firewall
	Denial of service (DDoS) protection
	Traffic anomaly protection
7.	**Management**
	Web based management to support for remote monitoring
	Accessible through variety of methods including: Telnet, Console Port, SSH
	Dedicated Out-of-Management interface
	Support SNMPv1, v2, v3 & Support for syslog
	Should have the ability to create customizable administrative roles/profiles (monitoring only, read-only accesses to configuration).
8.	**Software features**
	support for IPv4, RIPv2, OSPF, BGP, VLAN, DHCP, Support for IPv6 RIPng, OSPFv3.
9.	**Power Supply**
	Internal Redundant Power supply and redundant hot swappable fans

10.	**Minimum Interfaces Required**
	8 x 1 Gig and 8 x 10 Gig Ports loaded with required optics
	Router Should be EAL4/ NDPP/NDcPP certified

D	**Next Generation Fire Wall**
S. No	**Minimum Technical Specifications**
1.	**Architecture:**
	The appliance-based security platform shall be capable of providing firewall, IPS and VPN (IPSec) functionality simultaneously.
	The Firewall should have Application Security / AVC from Day 1.
	The Firewall should support Advanced Threat Protection like malware and zero-day threats through cloud subscription or should integrate with on premise APT solution
	Should provide Stateful failover.
	HA configuration that uses dedicated HA-control interfaces apart from the mentioned traffic interfaces
	Should provide active/active and active/standby failover
2.	**Sessions**
	Should support up to 1.5 Million Concurrent sessions and at least 50,000 sessions per second
3.	**System Throughput**
	Should provide 10Gbps IMIX throughput
	Should provide 2.6 Gbps IPS throughput
	Should have 1.5Gbps NextGen firewall throughput including Firewall, Application security/ AVC, IPS and URL Filtering
4.	**Support: -** IKEv1 and v2, IPSec VPN standards, 56-bit DES, 168-bit 3DES, 256-bit AES encryption
5.	**Authentication, Authorization and Accounting (AAA) support:** RADIUS or TACACS+
6.	**Support for:** Network and application-level attacks ranging from malformed packet attacks to DoS attacks, Support RSA and Diffie-Hellman, MD-5, SHA-1, SHA-128, SHA-256
7.	**Provides:**
	Rich dynamic NAT and PAT services
	Static NAT and PAT services
	Stateful and stateless and Zone-based firewall
	Denial of service (DDoS) protection
	Traffic anomaly protection
8.	**Management**

D	Next Generation Fire Wall
	Web based management to support for remote monitoring
	Accessible through variety of methods including: Telnet, Console Port, SSH
	Support SNMPv1, v2, v3 & Support for syslog
	Should have the ability to create customizable administrative roles/profiles (monitoring only, read-only accesses to configuration).
9.	**Software features**
	support for IPv4, RIPv2, OSPF, BGP, VLAN, DHCP, Support for IPv6 RIPng, OSPFv3.
10.	**Power Supply**
	Internal Redundant Power supply and redundant hot swappable fans
11.	**Minimum Interfaces Required**
	12 x 1G Port Accelerated ports and should have 4 free slots
	Firewall Should be EAL4/ NDPP/NDcPP certified

E	Tape Library with Robotic Arm – Minimum Technical Specifications	
Sr. No.	**Component**	**Minimum Technical Specifications**
1.	Feature	The Offered Tape Library must be with Minimum of two (2) LTO7 & one(1) LTO 9 FC tape drive (the latest) along with One (1) Robotic Arm. The Tape Library's drives must be scalable to 10 if required
2.	No. of Data Slots	The Offered Tape Library must be with minimum 500 cartridges slots and scalable to accommodate 1000 slots. This scalability should be with the addition of modules or frames.
3.	Tape Drive Architecture	The Tape Library must be Offered LTO7 drive and LTO 9 in the Library shall conform to the Continuous and Data rate matching technique for higher reliability.
4.	Speed	Offered LTO7 and LTO 9 drive shall support 300 MB/sec minimum in Native mode and 750 MB/sec in 2.5:1 Compressed mode or the best.
5.	Power Supply	The offered Tape Library must be offered with Redundant Power supply.
6.	Connectivity	The Offered Tape Library shall provide 8Gbps/higher native FC connectivity to SAN switches.
7.	Partitioning	Offered Tape Library must have partitioning support so that each drive can be configured in a separate partition. The Partioning License should be provided along with the Library.
8.	CARTRIDGES	MSI must Supply New Data cartridges & Cleaning Cartridges with barcode labels.
9.	Management	Tape Library shall provide web based remote management.

E	Tape Library with Robotic Arm – Minimum Technical Specifications	
10.	Encryption Keys	The offered tape library must support encryption and the encrypted keys should be managed by the ISV or the Tape library as an apart of solution i.e. The Data on the LTO media must be in Encrypted form, The Encryption management should be either AME or LME, to keep the keys safe and secured.
11.	Barcode Reader and Mail slots	Tape library shall support Barcode reader and min 2 mail slots- to deliver easy, secure access to individual tape cartridges without interrupting library operations.
12.	Other Features	1. Tape Library shall have GUI Panel
		2. Shall be rack mountable.
		3. The Tape library must Set alerts for backup and archive events. (Backup software shall manage these events)
		4. A 24x7 Comprehensive warranty for 1 year and AMC for 5 years or the best back-to-back with OEM - MAF TO BE provided.
		5. LCD front panel.

F	Minimum Technical Specifications for SAN Switch	
Sr. No.	**Feature**	**Minimum Technical Specifications**
1.	SAN ports and cables	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 48 Ports scalable to 96 ports. 48 No of 16Gbps SFP ports and 48 No of 15Mtr FC cable need to be populated
2.	Scalability	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only
3.	Architecture	Should deliver 16Gbit/Sec Non-blocking architecture with 1:1 performance for up to 96 ports in an energy-efficient manner
4.	Port Speed	Should protect existing device investments with autosensing 4, 8, and 16 Gbit/sec capabilities.
5.	Port Types	The switch shall support different port types such as FL_Port, F_Port, E_Port, EX_Port.
6.	Form Factor	The switch should be rack mountable
7.	Switch Features	Should provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN
		Non disruptive Microcode/ firmware Upgrades and hot code activation.
		The switch shall provide Aggregate bandwidth of 3072 Gbit/sec end to end.
		Switch shall have support for web-based management and should also support CLI.

F	Minimum Technical Specifications for SAN Switch	
		The switch should have USB port for firmware download, support save, and configuration upload/download.
		Offered SAN switches shall be highly efficient in power consumption. MSI shall ensure that each offered SAN switch shall consume less than 1000 Watt of power.
		Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).
		Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium, and low priority QOS zones to expedite high-priority traffic
		The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.
		SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.
		It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning
		The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.
		Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.

G	Minimum Technical Specifications for SAN Storage – Local Central Storage	
Sr. No.	**Feature**	**Specifications**
1.	Converge / Unified Storage	Offered Storage array shall be a true converge / unified storage with a single Microcode / operating system instead of running different Microcode / Operating system / Controllers for File, block, and object services respectively.
		Offered Storage array shall be end-to end 12Gbps enabled which means that both Front-end Fiber channel ports and Back-end engines shall be operated at minimum 12Gbps speed.
2.	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms including: *Windows 2012*, VMware, Solaris, HP-UX, IBM-AIX, Linux etc.
3.	Capacity & Scalability	The Storage Array shall be offered with 30 TB Raw capacity using SSD drives and 500 TB Raw capacity using SAS 10K Drives Storage shall be scalable to minimum of 300 Drives.

G	Minimum Technical Specifications for SAN Storage – Local Central Storage	
4.	Cache	Offered Storage Array shall be given with minimum of 64GB DRAM cache in a single unit and scalable to 128GB DRAM cache. OS overhead shall not be done inside cache.
		Offered Storage array shall also have additional support for Flash Cache using SSD / Flash drives. Both File services as well as Block operations shall be able to utilize flash cache. Minimum of 1200GB Flash cache shall be supported.
5.	Processing Power	Offered Storage architecture shall be based on purpose-built ASIC, XOR engine so that there shall be no load on the storage CPU during Raid Parity calculations. In case vendor doesn't have above ASIC functionality then additional 16GB read and write cache shall be provided per controller pair to balance the performance.
6.	Architecture & Processing Power	Controllers shall be true active-active so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc..
7.	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
8.	Disk Drive Support	Offered Storage Array shall support dual-ported 300 / 900 / 1200 / 1800GB hot-pluggable Enterprise SAS hard drives, Minimum of 400GB SSD Drives along with near line SAS drives of 2TB / 4TB / 6TB drives.
9.	Raid Support & Virtualization	Offered Storage Subsystem shall support Raid 0, 1, 1+0, 5, 50 and Raid 6, 60. Offered storage array shall have native virtualization support so that Raid 1. Raid 5, Raid 1+0, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application.
		Every supplied disk shall be able to participate into multiple and different raid sets simultaneously.
		In case vendor does not have above functionality, then 20% additional raw capacity shall be provided for each type of disk to balance out the capacity utilization.
10.	Data Protection	In case of Power failure, Storage array shall have de-stage feature to avoid any data loss.
11.	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, FCOE, SMB 3.0, NFS V4, NDMP etc.
12.	Host Ports and Back-end Ports	Minimum 8 no of 16Gbps FC front end ports scalable to 16 No of frontend ports. Minimum 1:1 front end vs back-end ratio for optimum performance needs to be provided. The storage should be scalable to 300Gbps frontend and 300Gbps Backend performance.

G	Minimum Technical Specifications for SAN Storage – Local Central Storage	
13.	Global Hot Spare	Offered Storage Array shall support distributed Global hot Spare for offered Disk drives. Global hot spare shall be configure as per industry practice.
14.	Performance and Quality of service	Shall have capability to use more than 30 drives per array group or raid group for better performance. Storage shall be provided with Performance Management Software.
		It should support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units.
		Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array.
		It shall be possible to change the quality-of-service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.
15.	Thin Provisioning and Space Reclaim	Array shall be supplied with Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity.
		Thin Re-claim (Zero Page reclaim) inside storage subsystem shall be automatic in nature and there shall be no need to run any utility inside storage for same.
		Thin Re-claim inside storage shall not cause any overloading of Storage CPU and shall be able to claim the Zero pages even during peak load without any performance impact
16.	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
17.	Snapshot / Point in time copy / Clone	Shall offered with snapshot and full copy (Clone) on the thin volumes if original volume is created on thick or vice-versa.
		The storage array should have support for both controller-based as well as file system-based snapshots functionality (At-least 1024 copies for a given volume or a file store). Storage array shall have functionality to re-claim the space from Thin Provisioned Deleted snapshot automatically.
18.	Quota Management and Antivirus Scanning	For file services operations, offered storage shall support both user level as well as file level hard and soft quota.
		For file services operations, offered storage shall support integration with industry leading antivirus vendors like Symantec and MacAfee.

G	Minimum Technical Specifications for SAN Storage – Local Central Storage	
19.	Storage Tiering	Shall be offered with dynamic migration of Volume from one Raid set to another set while keeping the application online.
		For effective data tiering, Storage subsystem shall support automatically Policy based Sub-Lun Data Migration from one Set of drive Tier to another set of drive tier.
20.	Remote Replication	Should support hardware-based data replication at the array controller level across all models of the offered family.
		The Storage array shall also support three ways (3 Data Centres) replication to ensure zero RPO in native fashion

H	Ingestion Server Minimum Technical Specifications	
Sr. No.	**Component**	**Minimum Technical Specifications**
1.	Ingestion Server	Minimum 2CPU Configuration, 1X Trusted Platform Module 2.0
2.	Processor	2 X Intel Xeon Silver 4208 Processor (2nd Gen) or Higher
3.	Processor Speed, Cache	11M Cache
4.	Chipset	Intel Chipset
5.	Memory	8 X 32GB RDIMM 2666MT/s Dual Rank BOSS controller card + with 2 M.2 Sticks 480GB.
6.	Hard Disk Drives	2 X 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR
7.	RAID Controller	Raid Controller 6G SAS/SATA HDD support. It should support RAID levels 0, 1,5,6,10.
8.	Ports	4 x USB 2.0, 1 VGA, and 1 Dedicated 1G Service LAN for Management (IPMI 2.0 Compliant).
9.	Drive bays	System should be configured with minimum 8 drive bays for installing Hard Drives. It should support SAS, SATA, and SSD Drives
10.	Graphics Controller	Integrated Graphic controller.
11.	Ethernet Ports	2 numbers of 1G Ethernet Port supporting PXE-Boot and iSCSI boot support and SAS port for connecting Tape Library.
12.	Expansion Slots	6 x PCI-Express 3.0 slots
13.	Optical Drive.	DVD-RW
14.	Fans	Fans should be redundant and hot plug.
15.	Redundant Power Supply	Hot swappable redundant (1+1) power supply or better.
16.	Operating System Support	Microsoft® Windows Server® 2012 R2 or above Windows 2008 R2, VMware vSphere 6.0, VMWare vSphere5.5, Suse Linux Ent Server11, RHEL7, RHEL 6, RHEL 5

H	Ingestion Server Minimum Technical Specifications	
17.	Virtualization software	VMWare vSphere Essentials Plus Kit - 6 Procs with 3 Years Basic Support
18.	FFMPEG Server	FFMPEG Server for proxy creation
19.	Management Software	Management software should have below features as standard or if any license is required for below features should be provided. • System management tools should be from the same OEM. • Should support Unattended, Local and Remote installation. • Event Management, Threshold management, Asset Management, Performance Management. • Prefailures and analysis, Automatic System Recovery and restart. • Monitoring and control power consumption • Raid Management, Storage management. • Update Management(Bios and Firmware), Online Diagnostics, • Single sign on and Role based access control should be provided. •Power Consumption Monitoring,Power Consumption Control should be provided. •Power Consumption history for at least 1 year should be available. Drivers and Firmware should be available for free till the complete life of the server.
20.	Compliance	ROHS, WEEE, CSAc/us, FCC Class A, CE, CB

I	Workstation Minimum Technical Specifications	
Sr. No.	**Component**	**Minimum Technical Specifications**
1.	Workstation	Intel Xeon W-2265 Processor or Higher
2.	Processor	2 X Intel Xeon Silver 4110 2.1G or Higher
3.	Chipset	Intel Chipset
4.	Memory	16GB x 4 DDR4-2933 MHz
5.	Hard Disk Drives	2TB SSD
6.	Graphics Controller	NVidia Quadro RTX 4000
7.	Expansion Slots	6 x PCI-Express 3.0 slots
8.	Optical Drive.	DVD-RW
9.	Fans	Fans should be redundant
10.	Operating System Support	Windows 10 Pro or higher

I	Workstation Minimum Technical Specifications	
11.	Keyboard and Accessories	Logic Keyboard Designed for Adobe Premier Pro CC
12.	Monitor	24-inch 1920x1200 WUXGA Monitor with HDMI Input / LCD Production Monitor
13.	Required Software	Blackmagic Design Deck link Studio 4K with HDMI output
14.	Compliance	ROHS

Other Requirements:

i. Other Office Accessories**:** other general IT accessories like Printer, Scanner etc. will also be part of the infrastructure. Supply of these accessories is not part of the scope for this RFP.

iii. Technical Specifications for Physical Components:

3.2. UPS

Reliability of electric power can affect operations of the Media Ingestion Room (MIR). Uninterrupted Power Supplies (UPS) shall be used to support the load of the critical components of the Media Ingestion Room (MIR)for periods of failure of the supplied electric power, while at the same time, filtering out transients. The scope shall include supply, transportation, storage, unpacking, erection, testing, successful commissioning, and satisfactory completion of trial operations of the above UPS systems for the Media Ingestion Room (MIR).

The UPS system should assure the MIR (Media Ingestion Room) equipment with continuous power at a solution uptime of 99.5% and with redundancy available up to the load end.

- Input Standard Voltage, 380 /400 / 415 V 3 Phase, 3 or 4 wire, +10 %, -15%
- Input Frequency, 50 Hz, +5% or -5%
- Output Steady State Voltage, 380 / 400 / 415 V +1% or -1%
- Output Frequency, 50 Hz, +0.25Hz to 0.5Hz
- Output Transient Voltage Stability, < 5% or –5% for a load change from 0% to 100%
- Overload – 125% for 10 minutes and 150% for 60 seconds
- Efficiency at full rated load, Not less than 92%

- Total Harmonic Content – With Linear Load < 2% for 100 % linear load and with 3:1 Crest factor load < 5%
- Input Harmonic Filter (for <10% Input current distortion)
- DC ripple (with & without Battery connected) < 1%
- Built In power factor correction
- Automatic shutdown of component for longer power outages
- Monitoring and logging the status of the power supply
- Displaying the voltage/current draw of the component
- Automatic restarting of component following a power outage
- Displaying the current voltage on the line
- Providing alarms on some error connections
- Providing protection against short circuits
- Operating Temperature range - 0 to 40 Celsius, Maximum 50 Celsius for 8 hrs.
- Design compliance with IEC and ISO
- Software that must be installed and integrated suitable operating system
- Supplies True Online UPS Power
- Non-Linear load compatible
- Capability to handle high Crest Factor load
- Ventilation- Air cooling with Integral Fans
- Built in Reliability & High Efficiency
- Low Audible Noise
- Compact Footprint
- Front Access for easy Maintenance
- The power factor of the UPS system shall be at 0.95 at all load conditions
- Input Current Harmonics < 10%
- The battery circuit breaker MCCB shall have O/L and U/V protection.

- The UPS shall have built in isolation transformer for re-referencing and to limit neutral-ground voltage to 1.50 volts by directly connecting dedicated earth to neutral of the output isolation transformer of the UPS as stipulated by server manufactures.

3.3. Diesel Generator Set

Diesel Engine – Diesel Engine, water cooled, Naturally Aspirated, developing 2 x 50 KVA BHP @ 1500 RPM, under NTP conditions of BS: 5514, with Dry Type Air Cleaner, Compact Radiator with Recovery Bottle and Pusher type Fan, Engine with Coolant, Engine mounted panel with wiring harness, Holset Coupling and Industrial Silencer, as per engine manufacturers design standards.

- Alternator – Standard design Alternator, rated at 0.8 PF, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, self-excited and self-regulated, with brushless excitation, Self- ventilated, Screen Protected Drip Proof, Insulation Class "H", enclosure IP 23. The A.C. Generator shall be Horizontal foot mounted single bearing type and shall be fitted with Automatic Voltage Regulator (AVR) for Voltage regulation of +/- 1% or better.
- Base Frame – Sturdy, fabricated, welded construction, channel iron Base Frame for mounting the above Engine and Alternator.
- Control Panel – Cubicle type, floor mounting Control Panel, with hinged doors, bottom gland plate and accommodating the following:
    - 1-No. ACB or Molded Case Circuit Breaker
    - 3-No.'s Ammeters /1 No. Ammeter with Selector Switch
    - 1 No. Voltmeter with Selector Switch
    - 1 No. frequency meter
    - 1 Set Pilot Lamps LOAD ON/GENERATOR ON
    - 1 Set Instrument Fuses
- Fuel Tank – Necessary liters capacity Fuel Tank with mounting brackets to run for

  8 hours, complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return. Diesel storage requirement for minimum 72 hours should be maintained
- Battery – Dry uncharged maintenance free batteries with leads and terminals.

- Management - The DG set should be manageable via Building Management System/ NOC with MODBUS Protocol with RS 485 Communication Port so that all software features like Diesel Consumption, Power, and Current etc. can be monitored on the BMS screen.

3.4. Civil & Architectural work

The scope for civil work in this RFP is to furnish the MIR (Media Ingestion Room)area in all aspects. The furnishing includes but not limited to the following

- Cement Concrete Work
- Cutting and chipping of existing floors
- Trench works
- Masonry works
- Hardware and Metals
- Glazing
- Paint work
- False Flooring
- False Ceiling
- Storage
- Furniture & fixture
- Partitioning
- Doors and Locking
- Painting
- Fireproofing all surfaces
- Insulating

The bidder should follow the civil and interior guidelines as mentioned below (The following specifications are indicative):

a. Raised Flooring

- Providing & fixing steel cementitious raised access floor of FFH Upto 450mm finished with antistatic high pressure laminate in size 600 x 600 mm x 35 mm with point load 450 kg and uniform distribution load (UDL) 1350 kg per sq. metre as per following specifications: Panel Type - M 1000, Under structure- Edge Support Rigid Grid, Wear resistance (g / cm2) - < 0.08, Bottom profile - Hemispherical shape, Pedestal -all steel construction & silver zinc plated, Exposed surface- Special weather coating on entire surface of the tiles. The same should also be provided with wire manager and tile lifter etc.

- At least 1' 6" High from existing floor level using antistatic laminated tiles.
- Supply & Fixing of 1.5 mm Antistatic Laminate skirting matching with floor tiles with 8mm thick MDF Board / Bison Board up to a height of 4".
- Supplying and fixing vinyl flooring with homogeneous flexible vinyl flooring of approved shade 2.0 mm thick in roll forms and manufacturers specification over the existing floor. Before laying, the existing flooring should be made free from dust and undulations. The finished flooring should be free from air bubbles and thoroughly cleaned without undulations.
- Providing and laying premium quality Granite white/ cream tiles of size 2'-0" x 2'-0", 8.5 mm thick set-in cement mortar and pointing with approved tile joint filler compound of approved make of matching shade as per manufacturer's specification as directed. The work shall include the preparation of base surface, cleaning, and acid wash.
- do - for skirting Upto a height of 4"
- Providing and fixing 9 mm thick floor insulation below the false flooring and joints should be finished properly as per manufacturer's specification.

b. False Ceiling

- Providing and fixing metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles and 25mm thick glass wool of 16kg.sq.m density wrapped on both sides with aluminium foil and placed over each tile etc.
- Providing and fixing 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. framework, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. Area of electrical fixtures will be paid full fixed to G.I. supports to receive spotlights including cutting hole etc., complete. G.I. metal frame to be of 24-gauge folded strip of 50mm width to be used. GI vertical supports to be anchored to slab by means of anchor fasteners.

c. Furniture and Fixture

- Workstation size of 2' depth made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. The desktop will be 25mm

thick & edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per design, complete with approved quality drawer slides, hinges, locks etc.

- Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate color outside and 2 coat of enamel paint inside the storage of size 1'6"x1'9"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish
- Cabin table of depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.
- Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low hit partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.
- Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate color outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.
- Fireproof safe (300 Ltr. or above) with one-hour fire rated.

d. Partitions

- Providing and fixing in position full height partition wall of 125 mm thick Fireline gyp-board partition using 12.5 mm thick double Fireline gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cutouts for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire-resistant coating.
- With glazing including the framework of 4" x 2" powder coated aluminum section complete (in areas like partition between server room & other auxiliary areas).
- Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft) wide.

e. Painting

- Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire-retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.
- For all vertical Plain surface.
- For Fireline gyp-board ceiling.
- Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Applying approved fire-retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

f. Civil Work

- Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement : 4 sand) with bricks of approved quality chamber bricks of class designation 50.
- Providing & making SS signage with text in etched & black painted of Line make or equivalent to be located as directed (wall mounted) for space nomenclature/ directions.
- Plastering with cement mortar 1:5 (1 cement: 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification.
- Anti-termite treatment of the entire critical area.

3.5. PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for nonmetallic conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths

of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.

- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and coarse sand.

3.6. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029 sq.mm. shall be used.
- Wherever wiring is run through Trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.

- Metal clad sockets shall be of dia cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts the earth continuity insulated copper wire in Green color shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required maximum number of PVC insulated 650 / 1100 grade copper conductor cable which can be drawn in a conduit.

3.7. Earthing

All electrical components are to be earthen is to by connecting two earth tapes from the frame of the component ring will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS- 3843-1986. The entire applicable IT infrastructure in the MIR shall be earthed.

- Earthing should be done inside the Media Ingestion Room (MIR)for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units etc. so as to avoid a ground differential. NFAI shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.
- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The earth connections shall be properly made. A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.

3.8. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary, the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a crisis crossing is avoided, and final take off to switch gear is easily facilitated.
- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that same they can be mounted on the wall.

- Whenever the rising mains pass through the floor, they shall be provided with a built-in fireproof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any crisscross wiring of the two, in order to avoid any interference, or corruption of data.
- The structured cabling for the MIR shall support Leaf & Spine switching architectures and be scalable and manageable in design to facilitate efficient installation and reporting. They should comprise of the following at a minimum:
    - The proposed cabling system should support at least 10G on Copper and up to 40G / 100G on fiber.
    - The fiber cabling should be of OM4+ or OM5 type and connectors and be scalable to managed system.
    - All cabling within the DC hall must be manageable using standard compliant centralized management system.
    - Dedicated copper trays and enclosed fiber pathway system to be considered for respective cable routing for the entire MIR.
- The cable pathway design must consider the cable fill ratio, separation, and bend limits as per TIA 569-C, ISO/IEC 14763-2:2012 and BICSI TDMM 13 design guidelines.

3.8. Precision Air Conditioning

The MIR shall be provided with fully redundant Microprocessor based Precision Air-conditioning system. Cool air feed to the MIR shall be bottom-charged or downward flow type using raised floor as supply plenum using perforated aluminum tiles for Air flow distribution. The return air flow shall be through false ceiling to cater to the natural upwardly movement of hot air. Cooling shall be done by the Precision Air-Conditioning system only. Forced cooling using Fans on False floor etc. is not acceptable. A/C should be capable of providing sensible cooling capacities at design ambient temperature & humidity with adequate airflow. The PAC should be capable to be integrated with the Building management System for effective monitoring.

The Agency will be required to design, supply, transport, store, unpack, erect, and test the successful commissioning and satisfactory completion of trial operations of the PAC systems for the Media Ingestion Room (MIR).This shall also include-

- Connecting the indoor unit with the mains electrical point
- Connecting indoor and outdoor units mechanically (with 18 G hard Gauge Copper piping).
- Connecting indoor and outdoor unit electrically.
- Nitrogen pressure testing, triple vacuum, final gas charging.
- Connecting the humidifier feed line with the point provided.
- Connecting the drain line with the point provided.
- Commissioning and handing over the unit to the customer.
- Operation and routine maintenance training to up to two persons nominated by the customer while commissioning the units at site

3.9. Temperature Requirements

The environment inside the MIR shall need to be continuously maintained at 12 ± 1° Centigrade. It is advised that the temperature and humidity be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24x7 basis and logged for providing reports.

3.10. Relative Humidity (RH) requirements

Ambient RH levels shall need to be maintained at 50% ± 5 non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.

3.11. Temperature & Relative Humidity Recorders

Temperature and Relative Humidity Recorders shall preferably be deployed for recording events of multiple locations within the MIR. Records of events for about past 7 days shall be recorded and presentable whenever required by NFAI. Automatic recording of temperature and humidity using sensors located at various locations within the MIR is necessary.

3.12. Air quality levels

The MIR shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The MIR shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat etc. Air filters shall be 95% efficiency & provide up-to 5 Micron particulate shall be deployed

Additional Points

- The precision air-conditioners should be capable of maintaining a temperature range of 12 degree with a maximum of 1-degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side.
- The precision air-conditioners shall have 2 independent refrigeration circuits (each comprising 1 no scroll compressors, refrigeration circuit and condensers) and dual blowers for flexibility of operations and better redundancy.
- The unit casing shall be in double skin construction for longer life of the unit and low noise level.
- For close control of the DC environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.
- The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.
- The internal rack layout design shall follow cold aisle and hot aisle concept as recommended by ASHRAE.
- The refrigerant used shall be environment friendly HFC, R-407-C/ equivalent in view of long-term usage of the MIR equipment's, availability of spares and refrigerant.
- Fully Deployed Dynamic Smart Cooling with Auto sequencing Provision and Auto Power Management Features
- Thermal and CFD Analysis diagrams should be provided
- The fan section shall be designed for an external static pressure of 25 Pa. The fans shall be located downstream of the evaporator coil and be of the electronically commuted backward curved centrifugal type, double width, double inlet and statically and dynamically balanced. Each fan shall be direct driven by a high efficiency DC motor.

- The evaporator coil shall be A-shape coil (for down flow) incorporating draw-through air design for uniform air distribution. The coil shall be constructed of rifled bore copper tubes and louvered aluminum fins, with the frame and drip tray fabricated from heavy gauge aluminum. Face area of coil shall be selected corresponding to air velocity not exceeding 2.5 m/sec.
- Dehumidification shall be achieved by either reducing effective coil area by solenoid valve arrangement or using Dew point method of control. Whenever dehumidification is required, the control system shall enable a solenoid valve to limit the exchange surface of the evaporating coil, thereby providing a lower evaporating temperature.
- The humidifier and heaters shall be a built-in feature in each machine individually. Humidification shall be provided by boiling water in a high temperature polypropylene steam generator. The steam shall be distributed evenly into the bypass airstreams of the environment control system to ensure full integration of the water vapor into the supply air without condensation. The humidifier shall have an efficiency of not less the 1.3 kg/kw and be fitted with an auto flush cycle activated on demand from the microprocessor control system. The humidifier shall be fully serviceable with replacement electrodes. Wastewater shall be flushed from the humidifier by the initiation of the water supply solenoid water valve via a U-pipe overflow system. Drain solenoid valves shall not be used. Microprocessor should be able to control the humidification and heating through suitable sensors
- Microprocessor Controls: Following features should be displayed on the units
    - Room temperature and humidity.
    - Supply fan working status
    - Compressor working status
    - Condenser fans working status
    - Electric heaters working status
    - Humidifier working status
    - Manual / Auto unit status
    - Line voltage value
    - Temperature set point
    - Humidity set point
    - Working hours of main component i.e., compressors, fans, heater, humidifier etc.
    - Unit working hours
    - Current date and time
    - Type of alarm (with automatic reset or block)

- The last 10 intervened alarms

- The microprocessor should be able to perform following functions
  - Testing of the working of display system
  - Password for unit calibration values modification
  - Automatic re-start of program
  - Cooling capacity control
  - Compressor starting timer
  - Humidifier capacity limitation
  - Date and time of last 10 intervened alarm
  - Start / Stop status storage
  - Random starting of the unit.
  - Outlet for the connection to remote system
  - Temperature and humidity set point calibration
  - Delay of General Alarm activation
  - Alarm calibration

- Following alarms shall be displayed on screen of microprocessor unit:
  - Air flow loss
  - Clogged Filters
  - Compressor low pressure
  - Compressor high pressure
  - Smoke - fire
  - Humidifier Low water level
  - High / Low room temperature
  - High/Low room humidity
  - Spare External Alarms
  - Water Under floor

- The control system shall include the following settable features:

- Unit identification number
- Startup Delay, Cold start Delay and Fan Run on timers
- Sensor Calibration
- Remote shutdown & general Alarm management
- Compressor Sequencing
- Return temperature control
- Choice of Modulating output types

- The unit shall incorporate the following protections:
  - Single phasing preventors
  - Reverse phasing
  - Phase misbalancing
  - Phase failure
  - Overload tripping (MPCB) of all components

3.13. Comfort Air Conditioning for Auxiliary Areas

- Capacity – 2 Tonnage
- Cooling Capacity – minimum 25000 BTU / Hr
- Compressor – Hermetically Sealed Scroll Type
- Refrigerant – R 22 Type
- Power Supply – Three Phase, 380-415 V, 50 Hz
- Air Flow Rate – minimum 19 cu m / min
- Noise Level - < 50 dB
- Operation – Remote Control

3.14. Fire Detection and Control Mechanism

Fire can have disastrous consequences and affect operations of a Media Ingestion Room (MIR). The early detection of fire and employing means for automatic suppression of the fire is important for effective functioning of a MIR.

System Description

- The Fire alarm system shall be an automatic 1-ton (e.g., 24) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.

- Detection shall be by means of automatic heat and smoke detectors located throughout the MIR(ceiling, false floor, and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

3.15. Control and indicating component

The control panel shall be a microprocessor based single loop addressable unit, designed, and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.

- All controls of the system shall be via the control panel only.
- All site-specific data shall be field programmable and stored in an integral EEPROM. The use of EPROM's requiring factory 'burning' and re-programming is not acceptable.
- All internal components of the control panel shall be fully monitored.
- The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.
- The system status shall be made available via panel mounted LEDs and a backlit 8-line x 40-character alphanumeric liquid crystal display.
- All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.
- Cancel fault and display test functions shall be configurable.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The control panel shall log a minimum of 700 events comprising of 100 event fire log and 200 event fault, disablement, and historic logs, giving time, date, device reference and status of indication.
- Fire, fault, and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display, and the internal supervisory buzzer.
- The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored, and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.

- All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.
- The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually, or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance reminder facility.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Enter or modify device text label
- Setup maintenance reminder
- Assign or modify zones
- Disable zones, device, sounders, FRE contact, auxiliary contacts
- Enable zones, device, sounders, FRE contact, auxiliary contacts
- Action weekly test
- Disable loop

Cable entries – The control panel will include the necessary top entry and rear entry cable entry points via 20mm knockouts.

Manual call points (MCP)

- MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS 5839: Part 2. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS 5839 Part 1 1988, without the need for special tools or the need to unfasten the cover plate.

- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. The device shall incorporate a short circuit isolation device and a red LED indicator.
- The MCP shall be suitable for surface or flush mounting. When flush mounted the device shall be capable of fixing to an industry standard single gang box.

Smoke detectors – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved.
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

Audible Alarms – Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.
- The labeling of Device and Zone labels should be part of the system.
- Necessary Software to the control panel

3.16. Fire Suppression Systems

The Clean Agent Fire Suppression system cylinder, approved seamless cylinders of global standards, discharge hose, fire detectors and panels and all other accessories required to provide a complete operational system meeting applicable requirements of NFPA 2001 Clean Agent Fire Extinguishing Systems, NFPA 70 National Electric Code, NFPA 72 National Fire Alarm Code or ISO standards must be considered to ensure proper performance as a system with UL/FM approvals and installed in compliance with all applicable requirements of the local codes and standards.

- The Clean Agent system considered for Total flooding application shall follow the provisions of Kyoto Protocol.
- Care should be taken that none of the Greenhouse Gases identified in the Kyoto Protocol is used for fire suppression application.
- The minimum criterion for the selection of the Clean Agent will be on the following parameters
    - Zero Ozone Depleting Potential.
    - Global Warming Potential not exceeding one.
    - Atmospheric Lifetime not exceeding one week.
- The clean agent fire suppression system with FK-5-1-12 and Inert Gas based systems are accepted as a replacement of HCFC and HFC as per Kyoto Protocol.
- The Clean Agent considered for the suppression system must be suitable for minable occupied areas with NOAEL Level (No observable adverse effect level) of 10% as compared to the design concentration to ensure high safety margin for the human who might be present in the hazard area.
- The minimum design standards shall be as per NFPA 2001, 2004 edition or latest revisions.
- Care shall be given to ensure proper early warning detection system with minimum sensitivity of 0.03% per foot obscuration as per NFPA 318 & NFPA 72 to ensure that one gets a very early warning to investigate the incipient fire much before the other detectors activate the fire suppression system automatically.
- All system components furnished and installed shall be warranted against defects in design, materials, and workmanship for the full warranty period, which is standard with the manufacturer, but in no case less than five (5) years from the date of system acceptance
- Additionally, Portable Extinguishers (CO_2 or Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the Media Ingestion Room (MIR) .

OR

- Fire suppression system shall deploy FM-200 (ETG-5) based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.
- Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm
- The OEM (/ Bidder) shall give a Certificate stating that their FM-200 system is approved by UL / FM / VdS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).
- The OEM (/ Bidder) shall also provide a Letter that the OEM has FM-200 Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill of materials and that such Software shall be type approved by FM / UL / VdS / LPC.
- The Storage Container offered shall be of Seamless type, meant for exclusive use in FM- 200 systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.
- The FM-200 valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.
- The FM-200 Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally tested for periodic servicing requirements and without any need to replace consumable parts.
- The individual FM-200 Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.
- The system flow calculation is to be carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VdS / LPC/ UL / FM.
- The system shall utilize 42 Bar / High pressure (600 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and also allow for better agent penetration in enclosed electronic equipment such as Server Racks/ Electrical Panels etc.

- The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the FM-200 system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.
- The suppression system shall provide for high-speed release of FM-200 based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 7% (v/v) of FM-200 for 21 degree Celsius or higher as recommended by the manufacturer.
- The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.
- Sub floor and the ceiling void to be included in the protected volume.
- The FM-200 systems to be supplied by the bidder must satisfy the various and all requirements of the Authority having Jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.
- The detection and control system that shall be used to trigger the FM-200 suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal, and start the pre-discharge condition.
- The discharge nozzles shall be in the protected volume in compliance to the limitation about the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VdS / LPC.
- The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the FM-200 containers.
- FM-200 shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.
- The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.
- The FM-200 discharge shall be activated by an output directly from the `FM-200' Gas Release control panel, which will activate the solenoid valve. FM-200 agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 600 psi (g) at 21°C with dry Nitrogen.

- The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.
- Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the FM-200 agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.
- The manual release device fitted on the FM-200 Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, FM-200 cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.
- FM-200 storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.
- FM-200 containers shall be equipped with a pressure gauge to display internal pressure.
- Brass Discharge nozzles shall be used to disperse the `FM-200'. The nozzles shall be brass with female threads and available in sizes as advised by the OEM system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.
- All the Major components of the FM-200 system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.
- Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.
- Release of FM-200 agent shall be accomplished by an electrical output from the FM-200 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.

3.17. High Sensitivity Smoke Detection System

General – The HSSD system shall provide an early warning of fire in its incipient stage, analyze the risk, and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly, and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

Regulatory Requirements

- National Electrical Code (NEC)

- Factory Mutual
- Local Authority having Jurisdiction

3.18. Access Control System

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Proximity as well as Biometric Technology for the critical areas and Proximity technology for non-critical areas. An access control system consisting of a central PC, intelligent controllers, proximity readers, power supplies, proximity cards and all associated accessories is required to make a fully operational online access control system. Access control shall be provided for doors. These doors shall be provided with electric locks and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts.

The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report, and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- Day, Date, Time, and duration-based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

3.19. CCTV System

The Media Ingestion Room (MIR) along with the Non-Critical area needs to be under constant video surveillance. The primary objective of implementing a CCTV system is to ensure effective surveillance of the area and also create a record for post event analysis. Monitoring cameras should be installed in proper areas to cover all the critical areas of the MIR. The scope of work involves supply, installation, commissioning, testing and maintenance of the Closed-Circuit Television system for Media Ingestion Room (MIR).

The CCTV system shall provide an on-line display of video images on monitor. The entire setup shall be monitored from the control room on 24/7 basis. Cameras with suitable lenses shall be used to view all the critical areas of the Media Ingestion Room (MIR), Reception and Corridor.

The CCTV system shall be based on the use of fixed dome cameras integrated dome cameras (fixed) and integrated pan/tilt/zoom cameras that can be controlled from control room location.

The CCTV System shall be a combination of color fixed and PTZ designed for continuous duty. The system and each of its devices shall be designed to meet the site ambient temperature and the site environmental conditions and shall operate satisfactorily under the specified permitted voltage and frequency variation band of the power supply source system.

All outdoor cameras shall be IP 66 rated.

The CCTV System proposed to fulfill the overall surveillance / Observation requirements and enhance the level of security necessary in a software establishment such as ours which shall be complete in all respects and shall comprise of following minimum items.

A set of fixed cameras, integrated dome cameras (fixed), pan / tilt / zoom (PTZ) cameras and integrated dome (PTZ) cameras with remote control operation of focus and zoom.

- A professional housing with internal and external cooling fans to protect both the camera and lens from the rigors of all environments and at the same time it should be designed and built for ease of installation and maintenance.
- A complete CCTV control facility that performs all the functions with provision to increase the total number of inputs for each monitor site.
- A complete system shall be connected through unshielded Twisted pair cable (UTP cable - Cat 6) as appropriate for the purpose establishing video and control of all cameras (fixed), pan / tilt / zoom (PTZ) cameras and integrated dome (PTZ)
- CCTV Cabinets as required complete with all cable termination facilities, cable distribution system for video and power system along with any additional video amplifiers and other video equipment as may be required.
- End point amplifiers as may be required to achieve satisfactory system operation.

- Test equipment covering all tools, tackles and testing equipment / kits as required for preventive and first line maintenance including test monitors, camera adjustment and testing facilities.
- Complete range of accessories as required.
- All necessary relay boxes connectors, extension cables and adapter boxes as required at each of the ends of the CCTV System as required.

General

- All systems and components shall have been thoroughly tested and proven in actual use.
- All systems and components shall be provided with a one-day turnaround repair express and 24-hour parts replacement. The manufacturer on warranty and non-warranty items shall guarantee the repair and parts expresses.
- Specifications included in this section are indicative and considered as a minimum; component and software that shall be acquired at the time of implementing the project shall be the latest versions available in the market.
- The system also should provide clear & accurate indication of an intruder or abnormal movement within and around the Facility.

System Capabilities

- The system shall provide visual images from the cameras located throughout the facility. The cameras located shall be fed into the Network Video Recorder (NVR) / Digital Video Recorder (DVR) located in the security room.
- The NVR / DVR shall support up to 32 channels with built-in recording system into Hard Disk
- The Main Security Control Room which shall house the Monitors and the Digital Video Management Server.
- The CCTV should be equipped with Digital recording facility for later scrutiny, with at least 90 days of recording facility.

Technical Requirements

3.20. Cameras

The cameras will be of 1/3" format CCD pickup device for fixed lens camera and ¼ "format for PTZ cameras. The cameras are being used for special observation purposes and are being located both indoor and outdoor & mounted on specially designed suitable mounting arrangement for operation under all severe environmental conditions to which these will be subjected especially the outdoor locations.

- The cameras being used at these locations shall have the following basic minimum requirements.
- The cameras shall be fixed, integrated dome (fixed) and the integrated Pan/Tilt/Zoom camera type that can be controlled from its monitor position, such that the cameras can be panned, tilted, zoomed, and focused on to any part or entire area which they have been located to bring under observation from keyboard location.
- The cameras shall be complete with the latest state of the art optical systems, filters, light sensitive pickup systems suitable for capturing images with very low light levels, and necessary interlaced scanners, encoders, decoders, associated amplifiers, synchronization facilities and any interfacing adapters as required, with all systems of that type suitable for a compact, durable, distortion free and clear image processing type camera.
- The color cameras (Integrated Pan/Tilt/Zoom dome) shall have a minimum resolution of 470 lines and sensitivity of 0.08 lux (color) and 0.013 lux (monochrome). The outdoor PTZ cameras shall be day/night camera with a minimum of 23 X optical zoom and 12 X digital zoom
- The Outdoor PTZ camera shall have a minimum of 80 X wide dynamic range, to withstand complex light variations in the environment.
- The preset accuracy for the camera shall be +/- 0.1degree maximum
- The Outdoor PTZ camera shall have a preset speed of 360 deg /sec Pan and 200 deg /sec tilt.
- The camera shall resume after alarm to the previously programmed state of alarm after alarm acknowledgement.
- The outdoor PTZ camera shall have auto flip feature, whereby which the dome shall rotate at 180 deg at the bottom of the tilt travel.
- The cameras shall have automatic level control complete with auto iris, and gain control of the amplifier and shall be complete with spot filter as required.
- The cameras shall have automatic shutter or 100% closing iris to prevent burning-in of image pickup device when the camera is not in use, both the shutter and iris shall fully close upon failure of power supply in order to prevent damage.
- The cameras shall have standby circuitry for when the camera is not selected on any of the monitors. The beam current of the camera pickup device shall be switched off automatically.
- The cameras shall have automatic circuitry which relates the black level in the signal to the darkest spot of the picture (black level control), limits the video signal in case of scene highlights in order to prevent overloading of the monitor (White limiter), and prevents the automatic sensitivity control from reacting to strong highlights (Peak white eliminator).

- The cameras shall have the features that shall prevent the occurrence of internal condensation or condensation on the window, necessary heaters/thermostats shall be provided as required.
- The cameras shall be equipped with Pan & Tilt heads to allow for rotation over a minimum 360 degrees.
- The cameras shall be provided with a local power distribution junction box, with local isolation switches and fuses to isolate each of the power circuits of the camera related to main camera power, and other circuits related to Pan & Tilt head, cooling fan, blower etc.
- The camera housing shall have a rain/sun shield and a weather protection feature with a minimum IP protection of IP66 for outdoor mounted cameras. For indoor cameras, the protection class shall be IP45.
- The aperture ratio (f-number) of the lenses shall be selected such that, a good picture is obtained at night.
- Power supply units, as required for the cameras, shall be provided.

Each of the CCTV cameras shall be located, mounted, positioned, and install such that:

- The camera and its supporting structures presence least obstruction of view and least obstruction for satisfactory movement and operation of the camera due to remote and local controls.
- The cameras shall not be mounted on vibrating structures, where this is not possible than special structures or other facilities/measures for reducing vibrations shall be provided.
- All the camera movements along with Pan and Tilt, and associated forces on structures are taken into account during the design and installation of the cameras.
- The installation presence the least risk of accidental damage.
- The equipment and its components are accessible for maintenance.
- The vibration of any object shall be less than that specified for the camera.

3.21. Monitors

There shall be total of 2 (27") monitors for each Digital Video Recorder one to view the multiplexed output second to view the switched . This monitor should be located in the main control room. The monitor shall be positioned such that room lights and windows are minimized.

The monitors may also be built into the control desk as appropriate.

Each of the monitors used at the main control room and operator status shall have the following basic minimum requirements.

- The monitor shall be suitable for use as desktop units.
- The monitors shall be high-resolution video monitors.
- The monitors shall have the facilities to loop the video signal through the other monitor.
- Each monitor shall have local control knobs and remote-control equipment and panel for monitor controls associated with power on/off switch standby on/off switch and for adjustment brightness, contrast, horizontal hold, vertical hold etc.
- Monitor shall be suitable for use as desktop units or can be rack mounted with suitable racks as appropriate.

3.22. Video & Telemetry Cables

The video signal shall be transmitted using co-axial cable and control of all zoom lens and Pan-Tilt functions through twisted pair interconnected between receiver and DVR.

Cabling for CCTV shall cover:

- Video link
- Remote control of cameras in terms of its control of pan tilts zooms & focus.
- Power supply cables.

The cable shall be shielded or provided with facilities to avoid interference between signals.

The transmission losses shall be minimized and where required for satisfactory operation correction amplifiers are cable equalizes shall be provided in the monitors on the CCTV cabinets.

3.23. Cabinets

CCTV cabinets shall be provided near set of monitors. The cable from the cameras shall be terminated in this cabinet from where these signals are distributed to the monitors.

All necessary video amplifiers, interfaces etc. that forms the part of the CCTV system shall be installed in the cabinet.

3.24. Dome Camera

The Dome camera unit shall be 1/3" CCD Colour Dome camera and shall provide a minimum of 540 TV lines resolution. It shall have built-in 3 -9mm varifocal lens. The camera shall operate on minimum lux level not more than 0.15 lux. The complete unit shall be housed in an integrated dome and base unit, both preferably made from injection moulded plastic. It shall be possible to adjust the camera head inside the dome in both the planes so that it can be wall and ceiling mounted. The camera shall operate on 24 V AC or 12 volts D.C.

3.25. Building Management System (BMS)

The building management system shall be implemented for effective management, monitoring, and Integration of various components like HVAC systems, Access Control systems, fire detection system etc.

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

- VESDA - Very Early Smoke Detection Apparatus
- Building Management & Control
- Data Collection & archival
- Alarm Event & Management
- Trending
- Reports & MIS Generation
- Maintenance & Complaint Management

The scope of work shall include designing supplying and installing of Building management (Automation) System. The work shall consist of furnishing all materials, equipment's, and appliances necessary to install the said system, complete with Sensors, Direct Digital Controllers, Communication Controllers and Supervisory Software complete with necessary software/hardware support for interfacing with other systems. It shall include laying of cabling duct, conduits, and power supply etc., necessary for installation of the system with supply of appropriate type products as indicated in the specification. The controller shall be 32-bit based Microprocessor Controller and shall sit directly on the TCP / IP network. The Controller shall be Web Based, Web Enabled, Real Time Clock, and Web Browser with Communication speed min of 10 Mbps.

Agency shall design & provide a full Building automation system on the basis of truly distributed intelligence and shall comprise of the following general functional sub systems.

- Air Conditioning Management & Control
  - Precision AC Units
  - Temperature monitoring and controls at all specified positions/locations
- Energy Management
  - LT Panel Energy Monitoring
  - UPS Monitoring
- Safety & Security Systems Integration
  - Fire Alarm System Integration
  - VESDA (Very Early Smoke Detection Alarm) System Integration
  - Access Control & Surveillance System Integration
  - Gas System Integration
- Integration
  - DG Set on MODBUS Protocol with RS 485 Communication Port
  - Energy Meter on MODBUS Protocol with RS 485 Communication Port

3.26. Water Leak Detection System

The water leak detector shall be installed to detect any seepage of water into the critical area and alert the Security Control Room for such leakage. It shall consist of water leak detection cable and an alarm module. The cable shall be installed in the ceiling & floor areas around the periphery.

- Water Leak Detection system should be for the Server and Network room Areas to detect and water flooding below the floor of the MIR.
- Water Leak Detection System should be wire based solution with alarm; the wire needs to lay in MIR surrounding the PAC units, which is the probable source of water leakage.

3.27. Common Alarm System

- The common alarm panel is required for checking the healthiness of all systems, to be installed at Media Ingestion Room.
- The panel can be installed in the Main Office of Phase – II.

The common alarm panel should have provision for accepting "potential free" signals from all system for relevant status change in that system

3.28. Electrical Panels

- The Panels shall be of compartmentalize design so that circuit arc / flash products do not create secondary faults and be fabricated out of high quality CRCA sheet, suitable for indoor installation having dead front operated and floor mounting type.
- All CRCA sheet steel used in the construction of Panels shall be 2 mm. thick and shall be folded and braced as necessary to provide a rigid support for all components. Joints of

any kind in sheet steel shall be seam welded, all welding slag grounded off and welding pits wiped smooth with plumber metal.

- The Panels shall be totally enclosed, completely dust and vermin proof and degree of protection being not less than IP: 54 to IS: 2147. Gaskets between all adjacent units and beneath all covers shall be provided to render the joints dust proof. All doors and covers shall be fully gasketed with foam rubber and /or rubber strips and shall be lockable.
- All panels and covers shall be properly fitted and secured with the frame and holds in the panel correctly positioned. Fixing screws shall enter into holes, taped into an adequate thickness of metal, or provided with bolts and nuts. Self-threading screws shall not be used in the construction of Panels.
- A base channel of 75 mm. x 50 mm. x 6 mm. thick shall be provided at the bottom.
- Panels shall be preferably arranged in multi-tier formation. The size of the Panels shall be designed in such a way that the internal space is sufficient for hot air movement. If necessary, openings shall be provided for natural ventilation, but the said openings shall be screened with fine weld mesh. The entire electrical component shall be dated for 50°c.
- The Panels shall be provided with removable sheet steel plates at top and bottom to drill holes for cable / conduit entry at site.
- The Panels shall be designed to facilitate easy inspection, maintenance, and repair.
- The Panels shall be sufficiently rigid to support the equipment without distortion under normal and under short circuit condition. They shall be suitably braced for short circuit duty

Circuit Compartments

- Each MCCB shall be housed in separate compartments and shall be enclosed on all sides. Sheet steel hinged lockable door shall be duty interlocked with the unit in `ON' and `OFF' position.
- All instruments and indicating lamp shall be mounted on the compartment door. Sheet steel barriers shall be provided between the tiers in a vertical section.

Instrument Compartments

- Separate adequate compartment shall be provided for accommodating instruments, indicating lamps, control contactors/ relays and control fuses etc.
- These components shall be accessible for testing and maintenance without any danger of accidental contact with live parts, bus bar and connections

3.29. Electrical Power and Control Wiring Connection

- Terminal for both incoming and outgoing cable connections shall be suitable for 1100 V grade, aluminum / copper conductor XLPE insulated, and PVC sheathed, armored cable and shall be suitable for connections of solder less sockets for the cable size as per the feeder capacity.
- Power connections for incoming feeders of the main Panels shall be suitable for 1100 V grade Aluminum conductor (XLPE) cables.
- Both control and power wiring shall be brought out in cable alley for ease of external connections, operation, and maintenance.
- Both control and power terminals shall be properly shrouded.
- 10% spare terminals shall be provided on each terminal block. Sufficient terminals shall be provided on each terminal block, so that not more than one outgoing wire is connected to per terminal.
- Terminal strips for power and control shall preferably be separated from each other by suitable barriers of enclosures.
- Wiring inside the modules for power, control, protection, and instruments etc. shall be done with use of 660 / 1100 V grade, FRLS insulated copper conductor cables conforming to IS. For current transformer circuits, 2.5 sq.mm. Copper conductor wire shall be used.
- Other control wiring shall be done with 1.5 sq.mm. Copper conductor wires.
- Wires for connections to the door shall be flexible. All conductors shall be crimped with solder less sockets at the ends before connections are made to the terminals.
- Control power supply to modules through the control transformer Control power wiring shall have control fuses, (HRC fuse type) for circuit protection. All indicating lamps shall be protected by HRC fuses.
- Particular care shall be taken to ensure that the layout of wiring is neat and orderly. Identification ferrules shall be filled to all the wire termination for ease of identification and to facilitate checking and testing

Terminals

- The outgoing terminals and neutral link shall be brought out to a cable alley suitably located and accessible from the panel front.
- The current transformers for instruments metering shall be mounted on the disconnecting type terminal blocks.
- No direct connection of incoming or outgoing cables to internal components of the distribution board is permitted; only one conductor may be connected in one terminal

Cable Compartments

- Cable compartments of minimum 300 mm size shall be provided in the Panels for easy termination of all incoming and outgoing cables entering from bottom or top.
- Adequate supports shall be provided in the cable compartments to support cables.
- All outgoing and incoming feeder terminals shall be brought out to terminals blocks in the cable compartment.

Labels

- Engraved PVC labels shall be provided on all incoming and outgoing feeders.
- Single line circuit diagram showing the arrangements of circuit inside the distribution board shall be pasted on inside of the panel door and covered with transparent laminated plastic sheet.

Name Plates

- A nameplate with the Panels designation in bold letters shall be fixed at top of the central panel.
- A separate nameplate giving feeder details shall be provided for each feeder module door.
- Inside the feeder compartments, the electrical components, equipment's, accessories like switchgear, control gear, lamps, relays etc. shall suitably be identified by providing stickers.
- Engraved nameplates shall preferably be of 3 ply, (Red-White-Red or Black-White-Black) lamicoid sheet. However, black engraved perplex sheet name plates shall also be acceptable. Engraving shall be done with square groove cutters.
- Nameplate shall be fastened by counter sand screws and not by adhesives

Danger Notice Plates

- The danger notice plate shall be affixed in a permanent manner on operating side of the Panels.
- The danger notice plate shall indicate danger notice both in Hindi and English and with a sign of skull and bones.
- The danger notice plates, in general, meet the requirements of local inspecting authorities.
- Overall dimensions of the danger notice plate shall be 200 mm. wide x 150 mm. high.

- The danger notice plate shall be made from minimum 1.6 mm. thick mild steel sheet and after due pre-treatment to the plate, the same shall be painted white with vitreous enamel paint on both front and rear surface of the plate.
- The letters, the figures, the conventional skull, and bones etc. shall be positioned on plate as per recommendation of IS : 2551-1982.
- The said letters, the figures and the sign of skull and bones shall be painted in signal red color as per IS: 5-1978.
- The danger plate shall have rounded corners. Location of fixing holes for the plate shall be decided to suit design of the Panels.
- The danger notice plate, if possible, it should be of ISI certification mark

3.30. Molded Case Circuit Breakers

- The molded case circuit breaker (MCCB) shall be air brake type and having quick make - quick break with trip free operating mechanism.
- Housing of the MCCB shall be of heat resistant and flame retardant insulating material.
- Operating handle of the MCCB shall be in front and clearly indicate ON/OFF/TRIP positions.
- The electrical contact of the circuit breaker shall be of high conducting non-deteriorating silver alloy contacts.
- The MCCB shall be provided microprocessor-based overload and short circuit protection device.
- All the releases shall operate on common trip busbar so that in case of operation of any one of the releases in any of the three phases, it will cut off all the three phases and thereby single phasing of the system is avoided.
- The MCCB shall provide two sets of extra auxiliary contacts with connections for additional controls at future date.

3.31. Contactors

- The contactors shall meet with the requirements of IS: 2959 and BS: 7755.
- The contactors shall have minimum making and breaking capacity in accordance with utilization category AC3 and shall be suitable for minimum Class II intermittent duty.
- If the contactor forms part of a distribution board then a separate enclosure is not required, but the installation of the contactor shall be such that it is not possible to make an accidental contact with live parts

3.32. Indicating Lamps

- Indicating lamps assembly shall be screw type with built in resistor having non-fading color lens. LED type lamps are required.
- Wiring for Remote ON, OFF, TRIP indicating lamp is required.
- Color shade for the indicating lamps shall be as below:
  - ON indicating lamp : Red
  - OFF indicating lamp : Green
  - TRIP indicating lamp : Amber
  - PHASE indicating lamp : Red, Yellow, Blue
  - TRIP circuit healthy lamp : Milky

4. Infrastructure available at NFAI

4.1. Hardware available at NFAI

#	Particulars	Quantity/ Size
1.	SAN Storage	100 TB
2.	LTO 7 tapes	9050 Nos.
3.	LTO 4 tapes	3250 Nos.
4.	Digibeta & Betacam	5500 Nos.
5.	U'matic tapes	3000 Nos.
6.	VHS	1500 Nos.

Note: The numbers mentioned above are indicative and are for providing a broad overview of the quantum at NFAI

4.2. Non-filmic Media files at NFAI

#	Particulars	Quantity
1	Wallposters	38,182

#	Particulars	Quantity
2	Song Booklets	22,228
3	Pamphlets	5,602
4	Stills	208,288
5	Slides	10,260
6	Press Clippings	199,360
7	**Total**	**483,920**

Note: The numbers mentioned above are indicative and are for providing a broad overview of the quantum at NFAI

4.3. Storage Sizing assumptions

Storage Sizing assumptions			
Content	**#**	**Type**	**Size (in TB)**
Features	2345	Access Copy	211.05
Shorts	2768	Access Copy	69.2
Previously Restored	578	Access Copy	38.47
10 Year projection for Born Digital Features to be put on OTT	5	Access Copy	45.18
Non-Filmic Content	725,000	Access Copy(.pdf)	32
Magnetic Tapes Digitization	10000	Access Copy	20
20% Buffer			83.18
Total Sizing Estimate (in TB)			**499.08**

Note: The numbers mentioned above are indicative and are for providing a broad overview of the quantum at NFAI

Chapter 7: Annexures

7.1. Checklist for the documents to be included in the Pre-Qualification Envelope

#	Eligibility Criteria	Document Proof	Submitted (Yes / No)	Proposal Pg. No
1.	Covering letter	As per the format mentioned in Chapter 7: Section 7.13		
2.	Bid processing fee	Demand Draft for Rs. 10,000		
3.	Bid Security Declaration format	As per the format mentioned in Chapter 7: Section 7.5		
4.	Power of Attorney authorizing the signing of the bid	As per the format mentioned in Chapter 7: Section 7.2		
5.	Power of Attorney for Prime Bidder of the Consortium	As per the format mentioned in Chapter 7: Section 7.3		
6.	Witness details and signatures for the Power of Attorneys	Note of Chapter 7: Section 7.2 and Section 7: Section 7.3		
7.	Power of Attorney is being issued. However, the Power of Attorney provided by Bidders from countries that have signed the Hague Legislation Convention 1961 are not required to be legalized by the Indian Embassy if it carries a conforming Apostille certificate.	Note of Chapter 7: Section 7.2 and Section 7: Section 7.3		
8.	PQ Criteria 2.1.1	Mention the document name here		
9.	PQ Criteria 2.1.2	Mention the document name here		

10.	PQ Criteria 2.1.3	Mention the document name here		
11.	PQ Criteria 2.1.4	Mention the document name here		
12.	PQ Criteria 2.1.5	Mention the document name here		
13.	PQ Criteria 2.1.6	Mention the document name here		
14.	PQ Criteria 2.1.7	Mention the document name here		

7.2. Power of Attorney for Authorization of A presentative for Signing of the Bid

<<On Rs. 500 Stamp paper>>

Know 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 / the Prime Bidder of our Consortium 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 bid for the …… Project proposed or being developed by the …… (the "Employer") including but not limited to signing and submission of all applications, bids and other documents and writings, participate in bidders' and other conferences and providing information / responses to the Employer, representing us in all matters before the Employer, signing and execution of all contracts and undertakings consequent to acceptance of our bid, and generally dealing with the Employer in all matters in connection with or relating to or arising out of our bid for the said Project and/or upon award thereof to us.

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 Notarized

(Signature, name, designation, and address of the Attorney)

Notes:

- The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required, the same should be under common seal affixed in accordance with the required procedure.
- Wherever required, the Bidder should submit for verification the extract of the charter documents and documents such as a board or shareholders resolution / power of attorney in favor of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Bidder.
- For a Power of Attorney executed and issued overseas, the document will also have to be legalized by the Indian Embassy and notarized in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Bidders from countries that have signed the Hague Legislation Convention 1961 are not required to be legalized by the Indian Embassy if it carries a conforming Apostille certificate.

7.3. Power of Attorney for Prime Bidder of Consortium

<<On Rs. 500 Stamp paper>>

Whereas the ……. (the "Employer") has invited bids from open market for the technically and financially qualified agencies and for the ……..... Project (the "Project").

Whereas ……., ……. and ……. (collectively the "Consortium") being Members of the Consortium are interested in bidding for the Project in accordance with the terms and conditions of the Request for Proposals and other connected documents in respect of the Project, and

Whereas it is necessary for the Members of the Consortium to designate one of them as the Prime Bidder with all necessary power and authority to do for and on behalf of the Consortium, all acts, deeds, and things as may be necessary in connection with the Consortium's bid for the Project and its execution. We also understand and accept that all members of the consortium shall be jointly and severally liable for the execution of the work.

NOW THEREFORE KNOW ALL MEN BY THESE PRESENTS

We, ……. having our registered office at ……., M/s. ……., having our registered office at ……., and M/s. ……., having our registered office at ……., (hereinafter collectively referred to as the "Principals") do hereby irrevocably designate, nominate, constitute, appoint, and authorize M/s ……., having its registered office at ……., being one of the Members of the Consortium, as the Prime Bidder and true and lawful attorney of the Consortium (hereinafter referred to as the "Attorney") and hereby irrevocably authorize the Attorney (with power to sub-delegate) to conduct all business for and on behalf of the Consortium and any one of us during the bidding process and, in the event the Consortium is awarded the Contract, during the execution of the Project, and in this regard, to do on our behalf and on behalf of the Consortium, all or any of such acts, deeds or things as are necessary or required or incidental to the submission of its bid for the Project, including but not limited to signing and submission of all applications, bids and other documents and writings, accept the Letter of Award, participate in bidders' and other conferences, respond to queries, submit information / documents, sign and execute contracts and undertakings

consequent to acceptance of the bid of the Consortium and generally to represent the Consortium in all its dealings with the Authority, and / or any other Government Agency or any

person, in all matters in connection with or relating to or arising out of the Consortium's bid for the Project and/ or upon award thereof is entered into with the Employer.

AND 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 / Consortium.

IN WITNESS WHEREOF WE THE PRINCIPALS ABOVE NAMED HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS …… DAY OF ……., 20.…

For

……...

(Signature, Name &

Title)

For …….....

(Signature, Name & Title)

For

……

(Signature, Name &

Title) (Executants)

(To be executed by all the Members of the Consortium)

Witnesses:

1.

2.

Notes:

- The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required, the same should be under common seal affixed in accordance with the required procedure. Wherever required, the Bidder should submit for verification the extract of the charter documents and documents such as a board or shareholders resolution/ power of attorney in favour of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Bidder.
- For a Power of Attorney executed and issued overseas, the document will also have to be legalized by the Indian Embassy and notarized in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Bidders from countries that have signed the Hague Legislation Convention 1961 are not required to be legalized by the Indian Embassy if it carries a conforming Apostille certificate.

7.4. Query Submission Format

Sr. No	Chapter	Section/ Sub Section	Page Number	Query

1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

7.5. Bid Security Declaration format

(On Company letterhead)

Date:_____ **Tender No. _____**

To ,

Officer on Special Duty,
National Film Heritage Mission,
National Film Archive of India, Law College Road,
Pune – 411 004.

Sir,

I/We. The undersigned, declare that:

I/We understand that, according to your conditions, bids must be supported by a Bid Security Declaration.

I/We accept that I/We may be disqualified from bidding for any contract with you for a period of one year from the date of notification if I am /We are in a breach of any obligation under the bid conditions, because I/We

a. have withdrawn/modified/amended, impairs, or derogates from the tender, my/our Bid during the period of bid validity specified in the form of Bid; or
b. having been notified of the acceptance of our Bid by the purchaser during the period of bid validity (i) fail or reuse to execute the contract, if required, or (ii) fail or refuse to furnish the Performance Security, in accordance with the Instructions to Bidders.

I/We understand this Bid Security Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the earlier of (i) the receipt of your notification of the name of the successful Bidder; or (ii) thirty days after the expiration of the validity of my/our Bid.

Sign

in the capacity of

Name:

Duly authorized to sign the bid for an on behalf of

Dated on _____ day of _____ (insert date of signing)

Corporate Seal

7.6. Performance Bank Guarantee

<<On Rs. 500 Stamp paper>>

To,

Officer on Special Duty,
National Film Heritage Mission,
National Film Archive of India, Law College Road,
Pune – 411 004.

Whereas <<name of the bidder / prime bidder and address>> (hereinafter called "the bidder") has undertaken, in pursuance of contract no. <Insert Contract No.> dated. <Date> to provide Implementation services for <<name of the assignment>> to NFAI (hereinafter called "the employer")

And whereas it has been stipulated by in the said contract that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract.

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the bidder, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the bidder to be in default under the contract and without cavil or argument, any sum, or sums within the limits of Rs. <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition, or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

a. Our liability under this Bank Guarantee shall not exceed Rs. <<Amount in figures>> (Rupees <<Amount in words>> only)
b. This Bank Guarantee shall be valid up to <<insert date>>)
c. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this Bank Guarantee that we receive a valid written claim or demand for payment under this Bank Guarantee on or before <<insert date>>) failing which our liability under the guarantee will automatically cease.

Authorized Signatory of the Bank)
Seal:

Date:

7.7. Details of the Single Entity / Prime Bidder

Sr.	Particulars	Details
1	Name and address	
2	Incorporation status of the firm (public limited / private limited partnership, LLP, etc.)	
3	Year of establishment	
4	ROC reference number (if applicable)	
5	Name, Address, email, Phone nos. and Mobile Number of Contact	

7.8. Project Citation Format

Relevant projects	
General information	
Name of the project	
Client for which the project was executed	
Name and contact details of the client	
Project details	
Description of the project	
Scope of services	
Service levels being offered	
Technologies used	
Outcomes of the project	
Other details	
Total cost of the project	
Total cost of the services provided by the bidder	
Duration of the project (no. of months, start date, completion date, current status)	

a. Copy of Work Order

b. Letter from the client to indicate the successful completion of the projects if any

7.9. Proposed Work Plan

#	Activity	Calendar Month					
		1	2	3	4	5	6

a. Indicate all main activities of the assignment, including delivery of reports (e.g.: inception, interim, and final reports), and other benchmarks. For phased assignments indicate activities, delivery of reports, and benchmarks separately for each phase.

b. Duration of activities shall be indicated in the form of a bar chart.

7.10. Team Composition

Name of Staff with qualification and experience	Area of Expertise	Position Assigned	Task Assigned	Time committed for the engagement

7.11. Format of CV for Key Personnel

PHOTOGRAPH				
Name				
Proposed Position				
Date of birth				
Years with Organization (if applicable)				
Nationality				
Education				
Degree (Specialization)	Institution			Year in which obtained
Relevant Certification (if any)				
Languages & degree of proficiency	Language	Read (Excellent/Good/ Fair)	Write (Excellent/Good/ Fair)	Speak (Excellent/Good /Fair)

Countries of work experience					
Employment record					
Employer	**From**	**To**			**Position held and Description of duties**
Detailed tasks handled (Domestic and International) (Work undertaken that best illustrates capability to handle the work and tasks assigned on this Project- Please give details of only those assignments that are relevant for the position for which the resource is being proposed)					
Customer Name	Brief Description of assignment	Role of resource	Start Date	End Date	Specific Task Allotted
Certifications					
I, the undersigned certify that:					
(i) To the best of my knowledge and belief, this CV correctly describes me, my qualifications, and my experience.					Yes/No
I understand that my willful misstatement described herein may lead to my disqualification or dismissal, if engaged.					
Name & Signature (Personnel)		Name & Signature (Authorized Representative)			
		Date of signing			

7.12. Financial Proposal Cover Letter

Date:

Officer on Special Duty,
National Film Heritage Mission,
National Film Archive of India, Law College Road,
Pune – 411 004.

Subject: Submission of the Commercial bid for Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution

Dear Sir,

We, the undersigned, offer to provide the services for <<Title of Implementation Services>> in accordance with your Request for Proposal dated <<Date>> and our Proposal (Technical and Commercial Proposals). Our attached Commercial Proposal is for the per unit sum of <<Rs……., Amount in words and figures>>. This amount is exclusive of all applicable taxes.

a. **PRICE AND VALIDITY**

   All the prices mentioned in our bid response are in accordance with the terms as specified in the RFP documents. We hereby confirm that our prices include all taxes. We understand that the actual payment would be made as per the existing indirect tax rates during the time of payment.

b. **UNIT RATES**

   We have indicated in the relevant forms enclosed, the unit rates and total amount for the purpose of account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

c. **COMPLIANCE**

   We declare that all the services shall be performed strictly in accordance with the bid documents, all of which have been detailed out exhaustively in the following statement, irrespective of whatever has been stated to the contrary anywhere else in our bid.

   Further we agree that additional conditions, if any, found in the bid documents, other than those stated in deviation schedule, shall not be given effect to.

d. TENDER PRICING

We further confirm that the prices stated in our bid are in accordance with your Scope of Work included in RFP documents

e. QUALIFYING DATA

We confirm having submitted the information as required by you in your bid document. In case you require any other further information/documentary proof in this regard before evaluation of our bid response, we agree to furnish the same in time to your satisfaction

f. BID PRICE

We declare that our Bid Price is for the entire scope of the work as specified in the <Refer Chapter No. >. These prices are indicated in the Commercial Bid attached with our Tender as part of the Tender.

g. PERFORMANCE BANK GUARANTEE

We hereby declare that in case the contract is awarded .to us, we shall submit the Performance Bank Guarantee (as per Chapter 7: Section 7.6:) of the RFP document

Our Commercial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal (Date)

We hereby declare that our bid response is made in good faith, without collusion or fraud and the information contained in the bid response is true and correct to the best of our knowledge and belief.

We understand that our bid response is binding on us and that you are not bound to accept bids you receive.

Thanking you,

Yours sincerely, Authorized Signature:

Name and Title of Signatory:

Name of Firm:_____

Address:_____

Note: The format provided in Chapter 4: section 8 shall be submitted along with the letter provided in this Chapter 7: Section 7.12 as part of financial proposal as provided in Chapter 3: Section 7.

7.13. Letter to be Submitted

<< On the letter head of the Prime Bidder>>

Dear ……,

a. The National Film Archive of India, Ministry of Information and Broadcasting, Government of India (hereinafter called "Employer") is executing the National Film Heritage Mission, NFHM.
b. The employer seeks to engage an Organization / Agency to provide services for "Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution"
c. More details of the services are provided in the Scope of Work in this RFP
d. An Organization / Agency will be selected under the Combined Quality Cum Cost Based System (CQCCBS) and procedures described in this RFP.
e. We understand that we have to inform in writing to "Officer on Special Duty, NFHM, National Film Archive of India, Law College Road, Pune", upon receipt:

i. That we have received the RFP document; and
ii. That we will submit the Proposal by the date & time indicated in the RFP

Yours sincerely, [insert: Signature, name, and title of Authorized Signatory]

7.14. Manufacturers Authorization Form (MAF)

(This form has to be provided by the OEMs of the products proposed)

Letter No.

Date:

To,

Officer on Special Duty,

National Film Heritage Mission,

National Film Archive of India, Law College Road,

Pune – 411 004.

Subject: OEM Authorization Letter

Ref: RFP from NFAI Ref: <RFP ref no> dated < date>

Dear Sir:

We who are established and reputable manufacturers / producers of having factories / development facilities at (address of factory / facility) do hereby authorize M/s (Name and address of Bidder / Prime Bidder) to submit a Bid and sign the contract with you against the above Bid Invitation.

We hereby extend our full guarantee and warranty for the Solution, Products and Services offered by the above firm against this Bid Invitation.

We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products manufactured or distributed by the Supplier:

a. Such Products as the Employer may opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract; and
b. In the event of termination of production of such Products:
    i. Advance notification to the Employer of the pending termination, in sufficient time to permit the Employer to procure needed requirements; and
    ii. Following such termination, furnishing at no cost to the Employer, the blueprints, design documents, operations manuals, standards, source codes and specifications of the Products, if requested.

We duly authorize the said bidder / prime bidder to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

Yours faithfully,

(Name)

(Name of Manufacturer)

Note: This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it in original.

7.15. Draft Contract Copy

General Conditions of Contract

7.15.1. general Provisions

1.1 Definitions

[Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

a) Applicable Law(s)" means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project; This also includes the relevant General Financial Rules and CVC Guidelines as directed by the Government from time to time. The Bidder shall abide by the same without raising any concerns

b) "Agency" means any private or public entity which has been awarded the LOA as per the provisions of the RFP, that will provide the Services to the "Employer" under the Contract.

c) "Contract" means the Contract signed by the Parties and all the attached documents listed in its Clause 1, which is this General Conditions (GC), the Special Conditions (SC), and the Appendices.

d) "Day" means calendar day.

e) "Effective Date" means the date on which this Contract comes into force and effect pursuant to Clause GC 2.1.

f) "Foreign Currency" means any currency other than the currency of the "Employer's" country.

g) "GC" means these General Conditions of Contract.

h) "Government" means the Government of India

i) "Local Currency" means Indian Rupees.

j) "Member" means any of the entities that make up the joint venture/consortium/association; and "Members" means all these entities.

k) "Party" means the "Employer" or the Agency, as the case may be, and "Parties" means both of them.

l) "Personnel" means professionals and support staff provided by the Agency or by any Sub-Agency and assigned to perform the Services or any part thereof; "Foreign Personnel" means such professionals and support staff who at the time of being so provided had their domicile outside the Government's country; "Local Personnel" means such professionals and support staff who at the time of being so provided had their domicile inside the Government's country.

and "Key Personnel" means the Personnel referred to in Clause GC 4.2(a).

m) "Reimbursable expenses" means all assignment-related costs [such as travel, translation, report printing, secretarial expenses, subject to specified maximum limits in the Contract].

n) "SC" means the Special Conditions of Contract by which the GC may be amended or supplemented.

o) "Services" means the work to be performed by the Agency pursuant to this Contract, as described in Appendix A hereto.

p) "Sub-Agency/s" means any person or entity to whom/which the Agency subcontracts any part of the Services.

q) "Third Party" means any person or entity other than the "Employer", or the Agency.

r) "In writing" means communicated in written form with proof of receipt.

1.2 Relationship between the Parties

Nothing contained herein shall be construed as establishing a relationship of master and servant or of principal and agent as between the "Employer" and the Agency. The Agency, subject to this Contract, has complete charge of Personnel and Sub- Agency/s, if any, performing the Services and shall be fully responsible for the Services performed by them or on their behalf hereunder.

1.3 Law Governing Contract:

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the applicable laws of India.

1.4 Headings: The headings shall not limit, alter, or affect the meaning of this Contract.

1.5 Notices

1.5.1 Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered post to such Party at the address specified in the SC.

1.5.2 A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified in the SC.

1.6 Location: The Services shall be performed at such locations as are specified in Appendix A hereto and, where the location of a particular task is not so specified, at such locations, as the "Employer" may approve

1.7 Authority of PRIME BIDDER/Lead Agency: In case the Agency consists of a consortium/ association of more than one entity, the Members hereby authorize the entity specified (Lead Agency) in the SC to act on their behalf in exercising all the Agency's rights and obligations towards the "Employer" under this Contract, including without limitation the receiving of instructions and payments from the "Employer". However, each member or constituent of Consortium of Agency shall be jointly and severally liable for all obligations of the Agency under the Contract.

1.8 Authorized Representatives: Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the "Employer" or the Agency may be taken or executed by the officials specified in the SC.

1.9 Taxes and Duties: The Agency, Sub-Agency/s and Personnel shall be liable to pay such direct and indirect taxes, duties, fees, and other impositions levied under the applicable laws of India.

1.10 Fraud and Corruption

1.10.1 Definitions: It is the Employer's policy to require that Employers as well as Agency observe the highest standard of ethics during the execution of the Contract. In pursuance of this policy, the Employer defines, for the purpose of this provision, the terms set forth below as follows:

(i) corrupt practice" means the offering, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the selection process or in contract execution.
(ii) "fraudulent practice" means a misrepresentation or omission of facts in order to influence a selection process or the execution of a contract.
(iii) "collusive practices" means a scheme or arrangement between two or more Agencies, with or without the knowledge of the Employer, designed to establish prices at artificial, noncompetitive levels.
(iv) "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process or affect the execution of a contract.

1.10.2 Measures to be taken by the Employer

(a) The Employer may terminate the contract if it determines at any time that representatives of the Agency were engaged in corrupt, fraudulent, collusive, or coercive practices during the selection process or the execution of that contract, without the Agency having taken timely and appropriate action satisfactory to the Employer to remedy the situation.
(b) The Employer may also sanction against the Agency, including declaring the Agency ineligible, either indefinitely or for a stated period of time, to be awarded a contract if it at any time determines that the Agency has, directly or through an agent, engaged in corrupt, fraudulent, collusive, or coercive
practices in competing for, or in executing, an Employer-financed contract.

1.10.3 Commissions and Fees

At the time of execution of this Contract, the Agency shall disclose any commissions or fees that may have been paid or are agreed to be paid to agents, representatives, or commission agents with respect to the selection process or execution of the contract. The information disclosed must include at least the name and address of the agent, representative, or commission agent, the amount and currency, and the purpose of the commission or fee.

2. COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

2.1 Effectiveness of Contract: This Contract shall come into force and effect on the date (the "Effective Date") of the "Employer's notice to the Agency instructing the Agency to begin carrying out the Services. This notice shall confirm that the conditions precedent and effectiveness conditions, if any, listed in the SC have been met.

2.2 Termination of Contract for Failure to Become Effective: If this Contract has not become effective within such time period after the date of the Contract signed by the Parties as specified in the SC 5, either Party may, by not less than twenty one (21) days written notice to the other Party, declare this Contract to be null and void, and in the event of such a declaration by either Party, neither Party shall have any claim against the other Party with respect hereto.

2.3 Commencement of Services: The Agency shall begin carrying out the Services not later than the number of days after the Effective Date specified in the SC 6.

2.4 Expiration of Contract: Unless terminated earlier pursuant to Clause GC 2.9 hereof, this Contract shall expire at the end of such time period after the Effective Date as specified in the SC 7.

2.5 Entire Agreement: This Contract contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any other statement, representation, promise or agreement not set forth herein.

2.6 Modifications or Variations:

(a) Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. Pursuant to Clause GC 7.2 here of, however, each Party shall give due consideration to any proposals for modification or variation made by the other Party.

(b) In cases of substantial modifications or variations, the prior written consent of the Employer is required.

2.7 Force Majeure

2.7.1 Definition

(a) For the purposes of this Contract, "Force Majeure" means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable and not brought about by or at the instance of the Party claiming to be affected by such events and which has caused the non-performance or delay in performance, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood or other extreme adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by Government agencies.

(b) Force Majeure shall not include

(i) any event which is caused by the negligence or intentional action of a Party or by or of such Party's Sub-Agencies or agents or employees, nor

(ii) any event which a diligent Party could reasonably have been expected both to take into account at the time of the conclusion of this Contract and avoid or overcome in the carrying out of its obligations hereunder.

(c) Subject to clause 2.7.2, Force Majeure shall not include Shall not include insufficiency of funds or inability to make any payment to fulfill any of its obligations for execution of the work shall not be considered to be a breach of, or default insofar as such inability arises from an event of Force Majeure, provided that the Bidder / Consortium member affected by such an event has taken all reasonable precautions, due care and reasonable alternative measures, all with the objective of carrying out the scope of work as mentioned in this RFP

2.7.2 No Breach of Contract: The failure of a Party to fulfill any of its obligations hereunder shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all reasonable precautions, due care, and reasonable alternative measures, all with the objective of carrying out the terms and conditions of this Contract.

2.7.3 Measures to be Taken: (a) A Party affected by an event of Force Majeure shall continue to perform its obligations under the Contract as far as is reasonably practical and shall take all reasonable measures to minimize the consequences of any event of Force Majeure. (b) A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible. (c) Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure. (d) During the period of their inability to perform the Services as a result of an event of Force Majeure, the Agency, upon instructions by the "Employer", shall either: (i) demobilize, or (ii) continue with the Services to the extent possible, in which case the Agency shall continue to be paid proportionately and on prorate basis, under the terms of this Contract. (e) In the case of disagreement between the Parties as to the existence or extent of Force Majeure, the matter shall be settled according to Clause GC 8.

2.8 Suspension: The "Employer" may, by written notice of suspension to the Agency, suspend all payments to the Agency hereunder if the Agency fails to perform any of its obligations under this Contract, including the carrying out of the Services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall allow the Agency to remedy such failure, if capable of being remedied, within a period not exceeding thirty (30) days after receipt by the Agency of such notice of suspension.

2.9 Termination

2.9.1.1. By the "Employer": The "Employer" may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (i) of this Clause GC 2.9.1.1

(a) If the Agency fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice of suspension pursuant to Clause GC 2.8 hereinabove, within thirty (30) days of receipt of such notice of suspension or within such further period as the "Employer" may have subsequently approved in writing.

(b) If the Agency becomes (or, if the Agency consists of more than one entity, if any of its Members becomes and which has substantial bearing on providing Services under this contract) insolvent or goes into liquidation or receivership whether compulsory or voluntary.
(c) If the Agency fails to comply with any final decision reached as a result of arbitration proceedings pursuant to Clause GC 8 hereof.
(d) If the Agency, in the judgment of the "Employer", has engaged in corrupt or fraudulent practices in competing for or in executing this Contract.
(e) If the Agency submits to the "Employer" a false statement which has a material effect on the rights, obligations, or interests of the "Employer".
(f) If the Agency places itself in position of conflict of interest or fails to disclose promptly any conflict of interest to the Employer.
(g) If the Agency fails to provide the quality services as envisaged under this Contract. The Employer shall formulate a Project Monitoring Committee (PMC) to monitor the progress of the assignment and the PMC may make judgment regarding the poor quality of services, the reasons for which shall be recorded in writing. The PMC may decide to give one chance to the Agency to improve the quality of the services.
(h) If, as the result of Force Majeure, the Agency is unable to perform a material portion of the Services for a period of not less than sixty (60) days.
(i) If the "Employer", in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

2.9.1.2 In such an occurrence the "Employer" shall give a not less than thirty (30) days' written notice of termination to the Agency, and sixty (60) days in case of the event referred to in (h).

2.9.2 By the Agency: The Agency may terminate this Contract, by not less than thirty (30) days' written notice to the "Employer", in case of the occurrence of any of the events specified in paragraphs (a) through (d) of this Clause GC 2.9.2.
(a) If the "Employer" fails to pay any money due to the Agency pursuant to this Contract and not subject to dispute pursuant to Clause GC 8 hereof within forty-five (45) days after receiving written notice from the Agency that such payment is overdue.
(b) If, as the result of Force Majeure, the Agency is unable to perform a material portion of the Services for a period of not less than sixty (60) days.

(c) If the "Employer" fails to comply with any final decision reached as a result of arbitration pursuant to Clause GC 8 hereof.
(d) If the "Employer" is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Agency may have subsequently approved in writing) following the receipt by the "Employer" of the Agency's notice specifying such breach.

2.9.3 Cessation of Rights and Obligations: Upon termination of this Contract pursuant to Clauses GC 2.2 or GC 2.9 hereof, or upon expiration of this Contract pursuant to Clause GC 2.4 hereof, all rights and obligations of the Parties hereunder shall cease, except (i) such rights and obligations as may have accrued on the date of termination or expiration, (ii) the obligation of confidentiality set forth in Clause GC 3.3 hereof, (iii) the Agency's obligation to permit inspection, copying and auditing of their accounts and records set forth in Clause GC 3.6 hereof, and (iv) any right which a Party may have under the Law.

2.9.4 Cessation of Services: Upon termination of this Contract by notice of either Party to the other pursuant to Clauses GC 2.9.1 or GC 2.9.2 hereof, the Agency shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum. With respect to documents prepared by the Agency and equipment and materials furnished by the "Employer", the Agency shall proceed as provided, respectively, by Clauses GC 3.9 or GC 3.10 hereof.

2.9.5 Payment upon Termination: Upon termination of this Contract pursuant to Clauses GC 2.9.1 or GC 2.9.2 hereof, the "Employer" shall make the following payments to the Agency:
(a) If the Contract is terminated pursuant to Clause 2.9.1 (g), (h) or 2.9.2, remuneration pursuant to Clause GC 6.3(h) (i)hereof for Services satisfactorily performed prior to the effective date of termination, and reimbursable expenditures pursuant to Clause GC 6.3(h)(ii) hereof for expenditures actually and reasonably incurred prior to the effective date of termination.
(b) If the agreement is terminated pursuant of Clause 2.9.1 (a) to (f), the Agency shall not be entitled to receive any agreed payments upon termination of the contract. However, the "Employer" may consider making payment for the part satisfactorily performed on the basis of

Quantum Merit as assessed by it if such part is of economic utility to the Employer. Applicable Under such circumstances, upon termination, the client may also impose liquidated damages as per the provisions of Clause 9 of this agreement. The Agency will be required to pay any such liquidated damages to client within 30 days of termination date.

2.9.6 Disputes about Events of Termination: If either Party disputes whether an event specified in paragraphs (a) through (g) of Clause GC 2.9.1 or in Clause GC 2.9.2 hereof has occurred, such Party may, within forty-five (30) days after receipt of notice of termination from the other Party, refer the matter to Clause GC 8 hereof, and this Contract shall not be terminated on account of such event except in accordance with the terms of any resulting arbitral award.

3. OBLIGATIONS OF THE AGENCY

3.1 General

Standard of Performance: The Agency shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency, and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Agency shall always act, in respect of any matter relating to this Contract or to the Services, as faithful adviser to the "Employer", and shall at all times support and safeguard the "Employer's legitimate interests in any dealings with Sub-Agency/s or Third Parties.

3.2 Conflict of Interests: The Agency shall hold the "Employer's interests paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments or their own corporate interests. If during the period of this contract, a conflict of interest arises for any reasons, the Agency shall promptly disclose the same to the Employer and seek its instructions.

3.2.1 Agency not to benefit from Commissions, Discounts, etc.: (a)The payment of the Agency pursuant to Clause GC 6 hereof shall constitute the Agency's only payment in connection with this Contract and, subject to Clause GC 3.2.2 hereof, the Agency shall not accept for its own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Contract or in the discharge of its obligations hereunder, and the Agency shall use its best

efforts to ensure that any Sub-Agency/s, as well as the Personnel and agents of either of them, similarly shall not receive any such additional payment. (b) Furthermore, if the Agency, as part of the Services, has the responsibility of advising the "Employer" on the procurement of goods, works or services, the Agency shall comply with the Employer's applicable procurement guidelines, and shall at all times exercise such responsibility in the best interest of the "Employer". Any discounts or commissions obtained by the Agency in the exercise of such procurement responsibility shall be for the account of the "Employer".

3.2.2 Agency and Affiliates Not to Engage in Certain Activities: The Agency agrees that, during the term of this Contract and after its termination, the Agency and any entity affiliated with the Agency, as well as any Sub-Agency/s and any entity affiliated with such Sub-Agency/s, shall be disqualified from providing goods, works or services (other than said scope of work services) resulting from or directly related to the Agency's Services for the preparation or implementation of the project.

3.2.3 Prohibition of Conflicting Activities: The Agency shall not engage and shall cause their Personnel as well as their Sub-Agency/s and their Personnel not to engage, either directly or indirectly, in any business or professional activities that would conflict with the activities assigned to them under this Contract.

3.3 Confidentiality: Except with the prior written consent of the "Employer", the Agency and the Personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Agency and its Personnel make public the recommendations formulated in the course of, or as a result of, the Services.

3.4 Insurance to be Taken out by the Agency: The Agency (i) shall take out and maintain, and shall cause any Sub-Agency/s to take out and maintain insurance, at their (or the Sub-Agency/s', as the case may be) own cost but on terms and conditions approved by the "Employer", insurance against the risks, and for the coverages specified in the SC9, and (ii) at the "Employer's request, shall provide evidence to the "Employer" showing that such insurance has been taken out and maintained and that the current premiums therefore have been paid.

3.5 Accounting, Inspection and Auditing: The Agency (i) shall keep accurate and systematic accounts and records in respect of the Services hereunder, in accordance with internationally

accepted accounting principles and in such form and detail as will clearly identify all relevant time changes and costs, and the bases thereof, and (ii) shall periodically permit the "Employer" or its designated representative and/or the Employer, and up to five years from expiration or termination of this Contract, to inspect the same and make copies thereof as well as to have them audited by auditors appointed by the "Employer" or the Employer, if so required by the "Employer" or the Employer as the case may be.

3.6 Agency's Actions Requiring "Employer's Prior Approval: The Agency shall obtain the "Employer's prior approval in writing before taking any of the following actions:

(a) Any change or addition to the Personnel listed in Appendix C.

(b) Subcontracts: The Agency may subcontract work relating to the Services to an extent and with such experts and entities as may be approved in advance by the "Employer". Notwithstanding such approval, the Agency shall always retain full responsibility for the Services. In the event that any Sub-Agency/s are found by the "Employer" to be incompetent or incapable or undesirable in discharging assigned duties, the "Employer" may request the Agency to provide a replacement, with qualifications and experience acceptable to the "Employer", or to resume the performance of the Services itself.

3.7 Reporting Obligations: The Agency shall submit to the "Employer" the reports and documents specified in Appendix B hereto, in the form, in the numbers and within the time periods set forth in the said Appendix. Final reports shall be delivered in CD ROM in addition to the hard copies specified in said Appendix.

3.8 Documents Prepared by the Agency to be the Property of the "Employer": All plans, drawings, specifications, designs, reports, other documents, and software prepared by the Agency for the "Employer" under this Contract shall become and remain the property of the "Employer", and the Agency shall, not later than upon termination or expiration of this Contract, deliver all such documents to the "Employer", together with a detailed inventory thereof. The Agency may retain a copy of such documents, but shall not use anywhere, without taking permission, in writing, from the Employer and the Employer reserves right to grant or deny any such request. If license agreements are necessary or appropriate between the Agency and third parties for purposes of development of any such computer programs, the Agency shall obtain the "Employer's prior written approval to such agreements, and the "Employer" shall be entitled at its

discretion to require recovering the expenses related to the development of the program(s) concerned.

3.9 Equipment, Vehicles and Materials Furnished by the "Employer": Equipment, vehicles and materials made available to the Agency by the "Employer" or purchased by the Agency wholly or partly with funds provided by the "Employer", shall be the property of the "Employer" and shall be marked accordingly. Upon termination or expiration of this Contract, the Agency shall make available to the "Employer" an inventory of such equipment, vehicles and materials and shall dispose of such equipment and materials in accordance with the "Employer's instructions. While in possession of such equipment, vehicles and materials, the Agency, unless otherwise instructed by the "Employer" in writing, shall insure them at the expense of the "Employer" in an amount equal to their full replacement value.

3.10 Equipment and Materials Provided by the Agencies: Equipment or materials brought into the Government's country by the Agency and the Personnel and used either for the Project or personal use shall remain the property of the Agency or the Personnel concerned, as applicable.

4. AGENCYS' PERSONNEL AND SUB-AGENCY/S

4.1 General: The Agency shall employ and provide such qualified and experienced Personnel and Sub-Agency/s as are required to carry out the Services.

4.2 Description of Personnel: (a) The title, agreed job description, minimum qualification, and estimated period of engagement in the carrying out of the Services of each of the Agency's Key Personnel are as per the Agency's proposal and are described in Appendix C. If any of the Key Personnel has already been approved by the "Employer", his/her name is listed as well.
(b) If required to comply with the provisions of Clause GC 3.1.1 hereof, adjustments with respect to the estimated periods of engagement of Key Personnel set forth in Appendix C may be made by the Agency by written notice to the "Employer", provided
(i) that such adjustments shall not alter the originally estimated period of engagement of any individual by more than 10% or one week, whichever is larger, and (ii) that the aggregate of such

adjustments shall not cause payments under this Contract to exceed the ceilings set forth in Clause GC 6.1(b) of this Contract. Any other such adjustments shall only be made with the "Employer's written approval.

(c) If additional work is required beyond the scope of the Services specified in Appendix A, the estimated periods of engagement of Key Personnel set forth in Appendix C may be increased by agreement in writing between the "Employer" and the Agency. In case where payments under this Contract exceed the ceilings set forth in Clause GC 6.1(b) of this Contract, this will be explicitly mentioned in the agreement.

4.3 Approval of Personnel: The Key Personnel and Sub-Agency/s listed by title as well as by name in Appendix C are hereby approved by the "Employer". In respect of other Personnel which the Agency proposes to use in the carrying out of the Services, the Agency shall submit to the "Employer" for review and approval a copy of their Curricula Vitae (CVs). If the "Employer" does not object in writing (stating the reasons for the objection) within twenty-one (21) days from the date of receipt of such CVs, such Personnel shall be deemed to have been approved by the "Employer".

4.4 Removal and/or Replacement of Personnel: (a) Except as the "Employer" may otherwise agree, no changes shall be made in the Personnel. If, for any reason beyond the reasonable control of the Agency, such as retirement, death, medical incapacity, among others, it becomes necessary to replace any of the Personnel, the Agency shall forthwith provide as a replacement a person of equivalent or better qualifications. (b) If the "Employer" (i) finds that any of the Personnel has committed serious misconduct or has been charged with having committed a criminal action, or (ii) has reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Agency shall, at the "Employer's written request specifying the grounds, therefore, forthwith provide as a replacement a person with qualifications and experience acceptable to the "Employer".

(c) Any of the Personnel provided as a replacement under Clauses (a) and (b) above, as well as any reimbursable expenditures (including expenditures due to the number of eligible dependents) the Agency may wish to claim as a result of such replacement, shall be subject to the prior written approval by the "Employer". The rate of remuneration applicable to a replacement person will be the rate of remuneration paid to the replacement person. Also, (i) the Agency shall bear all

additional travel and other costs arising out of or incidental to any removal and/or replacement, and (ii) the remuneration to be paid for any of the Personnel provided as a replacement shall not exceed the remuneration which would have been payable to the Personnel replaced.

4.5 Resident Project Manager: If required by the SC, the Agency shall ensure that at all times during the Agency's performance of the Services a resident project manager, acceptable to the "Employer", shall take charge of the performance of such Services.

5. OBLIGATIONS OF THE "EMPLOYER"

5.1 Assistance and Exemptions: Unless otherwise specified in the SC, the "Employer" shall use its best efforts to ensure that the Government shall:

a) Provide the Agency, Sub-Agency/s and Personnel with work permits and such other documents as shall be necessary to enable the Agency, Sub-Agency/s, or Personnel to perform the Services.

b) Arrange for the Foreign Personnel to be provided promptly with all necessary entry and exit visas, residence permits, exchange permits, and any other documents required for their stay in India.

c) Issue to officials, agents, and representatives of the Government all such instructions as may be necessary or appropriate for the prompt and effective implementation of the Services.

d) Provide to the Agency, Sub-Agency/s, and Personnel any such other assistance as may be specified in the SC.

5.2 Change in the Applicable Law Related to Taxes and Duties: If, after the date of this Contract, there is any change in the Applicable Laws of India with respect to taxes and duties, which are directly payable by the Agency for providing the services i.e. service tax or any such applicable tax from time to time, which increases or decreases the cost incurred by the Agency in performing the Services, then the remuneration and reimbursable expenses otherwise payable to the Agency under this Contract shall be increased or decreased accordingly by agreement between the Parties hereto, and corresponding adjustments shall be made to the ceiling amounts specified in Clause GC 6.1(b).

5.3 Services, Facilities and Property of the "Employer": (a) The "Employer" shall make available to the Agency and its Personnel, for the purposes of the Services and free of any charge, the services, facilities and property described in Appendix E at the times and in the manner specified in said Appendix E. (b) In case that such services, facilities and property shall not be made available to the Agency as and when specified in Appendix E, the Parties shall agree on any time extension that it may be appropriate to grant to the Agency for the performance of the Services.

5.4 Payment: In consideration of the Services performed by the Agency under this Contract, the "Employer" shall make to the Agency such payments and in such manner as is provided by Clause GC 6 of this Contract.

5.5 Counterpart Personnel: (a) If necessary, the "Employer" shall make available to the Agency free of charge such professional and support counterpart personnel, to be nominated by the "Employer" with the Agency's advice, if specified in Appendix E. (b) Professional and support counterpart personnel, excluding "Employer's liaison personnel, shall work under the exclusive direction of the Agency. If any member of the counterpart personnel fails to perform adequately any work assigned to such member by the Agency that is consistent with the position occupied by such member, the Agency may request the replacement of such member, and the "Employer" shall not unreasonably refuse to act upon such request.

6. PAYMENTS TO THE AGENCY

6.1 Total Cost of the Services

(a) The total cost of the Services payable is set forth in Appendix D as per the Agency's proposal to the Employer and as negotiated thereafter.

(b) Except as may be otherwise agreed under Clause GC 2.6 and subject to Clause GC 6.1(c), payments under this Contract shall not exceed the amount specified in Appendix-D.

(c) Notwithstanding Clause GC 6.1(b) hereof, if pursuant to any of the Clause's GC (c) or 5.2 hereof, the Parties shall agree that additional payments shall be made to the Agency in order to cover any necessary additional expenditures not envisaged in the cost estimates referred to in

Clause GC 6.1(a) above, the ceiling or ceilings, as the case may be, set forth in Clause GC 6.1(b) above shall be increased by the amount or amounts, as the case may be, of any such additional payments.

6.2 Currency of Payment: All payments shall be made in Indian Rupees. [In case the payment is to be made in the currency other that Indian Rupees, the same shall be mentioned instead of Indian Rupees]

6.3 Terms of Payment The payments in respect of the Services shall be made as follows:

(a) The Agency shall submit the invoice for payment when the payment is due as per the agreed terms. The payment shall be released as per the work-related milestones achieved and as per the specified percentage as per SC 13.

(b) Once a milestone is completed, the Agency shall submit the requisite deliverables as specified in this Contract. The Employer shall release the requisite payment upon acceptance of the deliverables. However, if the Employer fails to intimate acceptance of the deliverables or its objections thereto, within 30 days of receipt of it, the Employer shall release the payment to the Agency without further delay.

(c) **Final Payment:** The final payment as specified in SC 13 shall be made only after the final report and a final statement, identified as such, shall have been submitted by the Agency and approved as satisfactory by the "Employer". The Services shall be deemed completed and finally accepted by the "Employer" and the final report and final statement shall be deemed approved by the "Employer" as satisfactory ninety (90) calendar days after receipt of the final report and final statement by the "Employer" unless the "Employer", within such ninety (90) day period, gives written notice to the Agency specifying in detail deficiencies in the Services, the final report or final statement. The Agency shall thereupon promptly make any necessary corrections, and thereafter the foregoing process shall be repeated. Any amount, which the "Employer" has paid or caused to be paid in accordance with this Clause in excess of the amounts actually payable in accordance with the provisions of this Contract, shall be reimbursed by the Agency to the "Employer" within thirty (30) days after receipt by the Agency of notice thereof. Any such claim by the "Employer" for reimbursement must be made within twelve (12) calendar months after receipt by the "Employer" of a final report and a final statement approved by the "Employer" in accordance with the above.

(d) For the purpose of payment under Clause 6.3 (b) above, acceptance means; acceptance of the deliverables by the Employer after submission by the Agency and the Agency has made presentation to the PMC / Employer (Mention this if presentation is required) with / without modifications to be communicated in writing by the Employer to the Agency.

(e) If the deliverables submitted by the Agency are not acceptable to the Employer / PMC, reasons for such non-acceptance should be recorded in writing; the Employer shall not release the payment due to the Agency. This is without prejudicing the Employer's right to levy any liquidated damages under clause 9. In such case, the payment will be released to the Agency only after it re-submits the deliverable, and which is accepted by the Employer. All payments under this Contract shall be made to the accounts of the Agency specified in the SC.

(f) With the exception of the final payment under (c) above, payments do not constitute acceptance of the Services nor relieve the Agency of any obligations hereunder, unless the acceptance has been communicated by the Employer to the Agency in writing and the Agency has made necessary changes as per the comments/ suggestions of the Employer communicated to the Agency.

(g) In case of early termination of the contract, the payment shall be made to the Agency as mentioned here with: (i) Assessment should be made about work done from the previous milestone, for which the payment is made or to be made till the date of the termination. The Agency shall provide the details of persons reasonably worked during this period with supporting documents. Based on such details, the remuneration shall be calculated based on the man month rate as specified. (ii) A reasonable assessment of the reimbursable and miscellaneous expenses shall be made based on details furnished by the Agency in this regard with supporting documents and based on the assessment of the work done and the respective rates as provided. Wherever such an assessment is difficult, the rates should be arrived at by calculating the amount on pro-rata basis. The total amount payable shall be the amount calculated as per (i) and (ii) above plus any applicable tax.

7. FAIRNESS AND GOOD FAITH

7.1 Good Faith: The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

7.2 Operation of the Contract: The Parties recognize that it is impractical in this Contract to provide for every contingency which may arise during the life of the Contract, and the Parties hereby agree that it is their intention that this Contract shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Contract either Party believes that this Contract is operating unfairly, the Parties will use their best efforts to agree on such action as may be necessary to remove the cause or causes of such unfairness, but no failure to agree on any action pursuant to this Clause shall give rise to a dispute subject to arbitration in accordance with Clause GC 8 hereof.

8. SETTLEMENT OF DISPUTES

8.1 Amicable Settlement: Performance of the contract is governed by the terms & conditions of the contract, in case of dispute arises between the parties regarding any matter under the contract, Party of the contract may send a written Notice of Dispute to the other party. The Party receiving the Notice of Dispute will consider the Notice and respond to it in writing within 30 days after receipt. If that party fails to respond within 30 days, or the dispute cannot be amicably settled within 60 days following the response of that party, clause GC 8.2 shall become applicable.

8.2 Arbitration: In the case of dispute arising upon or in relation to or in connection with the contract between the Employer and the Agency, which has not been settled amicably, any party can refer the dispute for Arbitration under (Indian) Arbitration and Conciliation Act, 1996. Such disputes shall be referred to an Arbitral Tribunal consisting of 3 (three) arbitrators, one each to be appointed by the Employer and the Agency, the third arbitrator i.e., Presiding Arbitrator would be Joint Secretary (Films) in the Ministry of I&B.

8.3. Arbitration proceedings shall be held in Pune/Delhi in India at the place indicated in SC and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.

8.4 The decision of the majority of arbitrators shall be final and binding upon both parties. The expenses of the arbitrators as determined by the arbitrators shall be shared equally by the Employer and the Agency. However, the expenses incurred by each party in connection with the

preparation, presentation shall be borne by the party itself. All arbitration awards shall be in writing and shall state the reasons for the award.

9. Liquidated Damages

9.1 The parties hereby agree that due to negligence of act of any party, if the other party suffers losses, damages the quantification of which may be difficult, and hence the amount specified hereunder shall be construed as reasonable estimate of the damages and both the parties agree to pay such liquidated damages, as defined hereunder as per the provisions of this Contract.

The number of liquidated damages under this Contract shall not exceed [10] % of the total value of the contract as specified in Appendix D.

The liquidated damages shall be applicable under following circumstances:
(a) If the deliverables are not submitted as per schedule as specified in SC 13, the Agency shall be liable to pay 1% of the total cost of the services for delay of each week or part thereof.
(b) If the deliverables are not acceptable to the Employer as mentioned in Clause 6.3 (e), and defects are not rectified to the satisfaction of the Employer within 30 days of the receipt of the notice, the Agency shall be liable for Liquidated Damages for an amount equal to [0.5%] of total cost of the services for every week or part thereof for the delay.

10. Miscellaneous provisions:
(i) "Nothing contained in this Contract shall be construed as establishing or creating between the Parties, a relationship of master and servant or principal and agent.
(ii) Any failure or delay on the part of any Party to exercise right or power under this Contract shall not operate as waiver thereof.
(iii) The Agency shall notify the Employer/ the Government of India of any material change in their status, in particular, where such change would impact on performance of obligations under this Contract.
(iv) Each member/constituent of the Agency, in case of a consortium, shall be jointly and severally

liable to and responsible for all obligations towards the Employer/Government for performance of works/services including that of its Associates/Sub Agency/s under the Contract.

(v) The Agency shall at all times indemnify and keep indemnified the Employer/Government of India against all claims/damages etc. for any infringement of any Intellectual Property Rights (IPR) while providing its services under the Project.

(vi) The Agency shall at all times indemnify and keep indemnified the Employer/Government of India against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (the Agency's) employees or agents or by any other third Party resulting from or by any action, omission or operation conducted by or on behalf of the Agency.

(vii) The Agency shall at all times indemnify and keep indemnified the Employer/Government of India against any and all claims by Employees, Workman, Contractors, sub-contractors, suppliers, agent(s), employed engaged or otherwise working for the Contractor, in respect of wages, salaries, remuneration, compensation or the like.

(viii) All claims regarding indemnity shall survive the termination or expiry of the Contract.

(ix) It is acknowledged and agreed by all Parties that there is no representation of any type, implied or otherwise, of any absorption, regularization, continued engagement or concession or preference for employment of persons engaged by the (Agency) for any engagement, service, or employment in any capacity in any office or establishment of the Government of India or the Employer.

7.15.2. Special Conditions of Contract:

(Clauses in brackets {} are optional; all notes should be deleted in final text)

SC Clause	Ref. of G C	Amendments of, and Supplements to, Clauses in the Clause General Conditions of Contract
1.	1.5	The addresses are: 1. "Employer": Attention: Facsimile: 2. "Agency": Attention:

SC Clause	Ref. of G C	Amendments of, and Supplements to, Clauses in the Clause General Conditions of Contract
		Facsimile:
2.	1.7	{Lead Agency is [insert name of member]} Note: If the Agency consists of a consortium/ association of more than one entity, the name of the entity whose address is specified in above clause 1 should be inserted here. If the Agency consists only of one entity, this Clause should be deleted from the SC.
3.	1.8	The Authorized Representatives are: For the Employer: For the Agency:
4.	2.1	{The effectiveness conditions are the following: [insert conditions]} Note: List here any conditions of effectiveness of the Contract e.g., approval of the Contract by the Employer, "Employer's approval of Agency's proposals for appointment of specified key staff members, effectiveness of Employer Loan, receipt by Agency of advance payment and by "Employer" of advance payment guarantee (see Clause SC 6.4(a)), submission of performance security etc. If there are no effectiveness conditions, delete this Clause SC 2.1 from the SC.
5.	2.2	The time period shall be 30 days [insert time period, e.g.: four months].
6.	2.3	The time period shall be 7 days. [insert time period, e.g.: four months].
7.	2.4	The time period shall be 30 days [insert time period, e.g.: twelve months].
8.	3.4	Limitation of the Agency's Liability towards the "Employer" {Note: Proposals to introduce exclusions/limitations of the

SC Clause	Ref. of G C	Amendments of, and Supplements to, Clauses in the Clause General Conditions of Contract
		Agency's liability under the Contract should be carefully scrutinized by Employers/" Employer's. In this regard the parties should be aware of the Employer's policy on this matter which is as follows: 1. If the Parties agree that the Agency's liability should simply be governed by the Applicable Laws of India, they should delete this Clause SC 3.4 from the SC. If the Parties wish to limit or to partially exclude the Agency's liability to the "Employer", they should note that, to be acceptable to the Employer, any limitation of the Agency's liability should at the very least be reasonably related to (a) the damage the Agency might potentially cause to the "Employer", and (b) the Agency's ability to pay compensation using their own assets and reasonably obtainable insurance coverage. The Agency's liability should not be limited to less than a multiplier of the total payments to the Agency/s under the Contract for remuneration and reimbursable expenses. A statement to the effect that the Agency/s are liable only for the re- performance of faulty Services is not acceptable to the Employer. Also, the Agency's liability should never be limited for loss or damage caused by the Agency's gross negligence or willful misconduct.
9.	3.4	The risks and the insurance coverage shall be as follows: (Note: Delete/modify whichever is not applicable) (a) Third Party motor vehicle liability insurance in respect of motor vehicles operated in the Government's country by the Agency or its Personnel or any Sub- Agency/s or their Personnel, with a minimum coverage of [insert amount and currency].

SC Clause	Ref. of G C	Amendments of, and Supplements to, Clauses in the Clause General Conditions of Contract
		(b)Third Party liability insurance, with a minimum coverage of [insert amount and currency]. (c)Professional liability insurance to cover the employer against any loss suffered by the employer due to the professional service provided by the Agency, with a minimum coverage of [insert amount and currency]. (d)Workers' compensation insurance in respect of the Personnel of the Agency and of any Sub-Agency/s, in accordance with the relevant provisions of the Applicable Laws of India, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate; and (e)Insurance against loss of or damage to (i) equipment purchased in whole or in part with funds provided under this Contract, (ii) the Agency's property used in the performance of the Services, and (iii) any documents prepared by the Agency in the performance of the Services, by theft, fire, or any natural calamity. Note: If there are no other actions, delete this Clause SC 3.6
10.	4.5	{The person designated as resident project manager in Appendix C shall serve in that capacity, as specified in Clause GC 4.6.} Note: If there is no such manager, delete this Clause SC 4.6.
11.	5.1	Note: List here any changes or additions to Clause GC 5.1. If there are no such changes or additions, delete this Clause SC
12.	6.1 b	The ceiling in local currency is: [insert amount and currency]
13.	6.3	[Delete whichever is not applicable]

SC Clause	Ref. of G C	Amendments of, and Supplements to, Clauses in the Clause General Conditions of Contract
		In accordance with Chapter 5:Section 1 of RFP
14.	8.3	The Arbitration proceedings shall take place in courts of Pune/Delhi (indicate name of the city) in India.

Binding signature of Employer Signed by

(for and on behalf of the President of India)

Binding signature of Agency Signed by

(for and on behalf of ____ duly authorized vide Resolution No_____ dated _____ of the Board of Directors of _____)

In the presence of

(Witnesses)

1.

2.

7.15.3. Appendices

APPENDIX A – DESCRIPTION OF SERVICES

Note: This Appendix will include the final Terms of Reference worked out by the "Employer" and the Agency/s during technical negotiations, dates for completion of various tasks, place of performance for different tasks/activities, specific tasks/activities/outcome to be reviewed, tested, and approved by "Employer", etc.

APPENDIX B - REPORTING REQUIREMENTS

Note: List format, frequency, and contents of reports; persons to receive them; dates of submission; etc. If no reports are to be submitted, state here "Not applicable."

APPENDIX C – STAFFING SCHEDULE

(Include here the agreed (negotiated staffing schedule including the engagement of sub-contractors, if any)

APPENDIX D – Total COST OF SERVICES (in INR)

(Include here the rates quoted in the Commercial proposal or the negotiated rates, whichever is applicable)

APPENDIX E - DUTIES OF THE "EMPLOYER"

(Include here the list of Services, facilities, and property to be made available to the Agency by the "Employer").

****

7.16. Letter to be Submitted

<< On the letter head of the Prime Bidder>>

Dear ……,

1. The National Film Archive of India, Ministry of Information and Broadcasting, Government of India (hereinafter called "Employer") is executing the National Film Heritage Mission, NFHM.
2. The employer seeks to engage an Organization / Agency to provide services for "Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution."
3. More details of the services are provided in the Scope of Work in this RFP
4. An Organization / Agency will be selected under the Combined Quality Cum Cost Based System (CQCCBS) and procedures described in this RFP.
5. The RFP includes the following documents:
    a. Chapter 1 – Invitation of Bids
    b. Chapter 2 – Scope of Work
    c. Chapter 3 – Instruction to Bidders
    d. Chapter 4 – Evaluation Process
    e. Chapter 5 – Delivery Schedule & Payment Milestones
    f. Chapter 6 – Technical Specifications
    g. Chapter 7 – Annexure
6. We understand that we have to inform in writing to "Officer on Special Duty, NFHM, National Film Archive of India, Law College Road, Pune", upon receipt:
    a. That we have received the RFP document; and
    b. That we will submit the Proposal by the date & time indicated in the RFP

Yours sincerely,

[insert: Signature, name, and title of Client's representative]

7.17. Certificate of compliance by the Prime bidder and its associated parties

<<On Company letterhead>>

Certificate of Compliance to Government Orders

Date: _____

This is to inform that, M/s_____ (Prime bidder),M/s_____ (Consortium member(s)), M/s _____ (International Knowledge Partner(s)) and M/s_____ (Manufacturer(s) whose software, hardware, equipment and any other item(s) are proposed in the technical bid of M/s _____(Prime bidder) are in compliance with order F. No. 6/18/2019-PPD issued by Department of Expenditure via Office Memorandum dated July 23, 2020.

We, M/s_____(Prime bidder) and M/s _____(Consortium member(s)) understand and accept that if such certification is found to be false, it would be a ground for immediate termination and further legal action in accordance with relevant laws of Government of India.

Name of Authorized signatory: _____

Signature of authorized signatory: _____

Stamp of the Organization (Prime bidder and Consortium member(s))

7.18. Undertaking - Technical Support Arrangement with OEM

<< To be printed on Bidder/ Lead Bidder Company's Letter Head, signed by Authorized Signatory>>

Tender No.: Date:

To,

Officer on Special Duty,

National Film Heritage Mission,

National Film Archive of India, Law College Road,

Pune – 411 004.

Dear Sir,

Subject: RFP for Selection of Master System Integrator (MSI) for Implementation of NFAI's Enterprise Solution - Technical Support Arrangement with OEM

We, the undersigned, having read and examined the requirements of the project, have licensed all our products / COTS that shall complement the solution in the best possible way and that all the business and functional requirements shall be fulfilled either by the products/COTS or through customizations.

We have/shall enter(ed) into requisite arrangements with the OEMs for the following:

- **Professional Services and Technical Support:** We confirm that we have chosen the products from OEMs who have professional support services in India (or through their authorized channel partners) as per requirements of the RFP. These professionals shall be made available physically as and when required for supporting all technical aspects of project implementation, solution maintenance and support during entire period of Project including extended period if any as stated in RFP.
- **Vetting of solution**: We confirm that OEM's support shall be taken for vetting of the technical solution as proposed and implemented.

It is hereby confirmed that I/We are entitled to act on behalf of our company and empowered to sign this document as well as such other documents, which shall be required in this connection.

Summary of Arrangement with OEMs for implementation and operations support

S. No.	OEM Name and Registered Office	Product	Arrangement for Technical Support

(Signature of the Authorized signatory of the Bidder)
Name:
Designation:
Seal:
Date:
Place:
Business Address: