Directorate of Forensic Science Services
Ministry of Home Affairs, Govt of India
Block No. 09, 8th Floor, CGO Complex
New Delhi 110003

EXPRESSION OF INTEREST (EOI) - ESTABLISHMENT OF NATIONAL FORENSIC DATA CENTRE (NFDC)

The Directorate of Forensic Science Services (DFSS), Ministry of Home Affairs, Govt. of India, is intended to invite proposals from eligible vendors for implementing and managing a Turnkey Project to establish the National Forensic Data Centre (NFDC) for Forensic Indices. The EOI aims to understand bidders' capabilities in delivering a scalable, sustainable, and technically robust solution for this critical national initiative. NFDC will be a centralized national repository that integrates forensic data using Forensic Data Management System across multiple Forensic Indices not limited to; DNA, Ballistics, Handwriting, Face, Voice, and Narcoticssourced initially from Seven (07) Central Forensic Science Laboratories (CFSLs) at Delhi, Chandigarh, Hyderabad, Kolkata, Bhopal, Guwahati and Pune, later to be extended to more Central and State FSLs. The NFDC aims to enable seamless enrolment, search, matching, and verification of forensic questioned data with reference data of forensic indices.

The vendors are allowed to participate for single or multiple forensic indices and/or for complete system integration of all indices, software and Hardware storage. The eligible and interested vendors willing to participate against this EOI can access the complete technical requirements/information from the DFSS website:http://dfs.nic.in/downloads. The proposal may be reached to this Directorate within Twenty One (21) days of publication of this EOI. Proposals received after the due date will not be considered by this Directorate.

Sd/-
(D V Subrahmanyam)
Assistant Director (Admn.)

Place: New Delhi

Dated: June 6, 2025

Technical Document in r/o Expression of Interest for Establishment of National Forensic Data Center (NFDC)

By

Directorate of Forensic Science Services
Ministry of Home Affairs,
Government of India
8th Floor, Block No. 9,
CGO Complex, Lodhi Road,
New Delhi- 110003.

http://dfs.nic.in/

Disclaimer

The information presented in this Expression of Interest (EOI) document, or subsequently communicated to Bidders—whether orally, in writing, or in any other form—by or on behalf of the Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India (DFSS), or its employees or advisors, is shared subject to the terms and conditions outlined herein.

This EOI does not constitute a contract, nor does it represent an offer or invitation by DFSS to any potential Bidder or other party. Its sole purpose is to provide interested parties with information that may assist them in preparing their proposals in response to this EOI. The assumptions, assessments, statements, and information contained in this document may not be exhaustive, accurate, adequate, or correct. Therefore, each Bidder is advised to conduct its own examinations and analysis, and to independently verify the accuracy, adequacy, reliability, and completeness of the information provided. Bidders are also encouraged to seek independent professional advice as appropriate.

Neither DFSS nor its employees or advisors shall be liable to any person, including any Bidder, under any law, statute, regulation, or in tort, contract, or otherwise, for any loss, damage, cost, or expense arising from or related to the use of this EOI or any information contained herein - including, but not limited to, the accuracy, adequacy, reliability, or completeness of the EOI.

DFSS reserves the right, at its sole discretion and without any obligation, to update, amend, or supplement the information, assessments, or assumptions contained in this EOI. The release of this EOI does not imply any commitment by DFSS to select a Bidder or appoint a Selected Bidder for the project. DFSS further reserves the right to reject any or all proposals without providing any reason.

All costs incurred by the Bidder in connection with the preparation and submission of their proposal—including, but not limited to, preparation, copying, postage, delivery, expenses related to demonstrations or presentations requested by DFSS, and any other associated costs—shall be borne solely by the Bidder.

The primary objective of this EOI is to select a successful bidder from among the participating vendors for the National Forensic Data Center (NFDC) initiative. The specific goals of this EOI are as follows:

a. To invite proposals from vendors for providing comprehensive “Turnkey Project & Bundled Services” for the implementation and management of the NFDC.
b. To understand how vendors intend to meet the technical and operational requirements of the NFDC.
c. To assess vendors’ strategies for delivering services and supporting the ongoing demand and growth of requirements.
d. To evaluate vendors’ approaches for ensuring the scalability and upgradability of the proposed infrastructure and solutions.

The Directorate of Forensic Science Services (DFSS)/Ministry of Home Affairs (MHA) have the sole authority to select the shortlisted (successful) bidder through this EOI process. The decision of DFSS regarding the selection of the successful bidder shall be final, and DFSS reserves the right to reject any or all bids without assigning any reason.

1. Introduction

The Directorate of Forensic Science Services (DFSS), under the Ministry of Home Affairs (MHA), has envisioned the creation of the National Forensic Data Centre (NFDC). This initiative is designed to address the critical need for a centralized forensic database at the national level. The NFDC will consolidate forensic data initially from all Seven (07) Central Forensic Science Laboratories (CFSLs), at Delhi, Chandigarh, Hyderabad, Kolkata, Bhopal, Guwahati and Pune, later to be extended to more Central and State FSLs, leveraging forensic indices of criminals across various disciplines, not limited to; DNA, Ballistics, Handwriting, Face, Voice and Narcotics.

The primary objective is to establish a unified criminal database of Forensic Indices that integrates available evidence and information from all Seven (07) CFSLs, with the flexibility to incorporate additional forensic disciplines in the future as requirements evolve. The NFDC will facilitate the enrolment of criminal forensic indices, with identification authenticated by respective CFSLs. This centralized system will enable individual CFSLs and forensic experts to enable seamless enrolment, search, matching, and verification of forensic questioned data with reference data of forensic indices.

Additionally, the NFDC will provide need-based access to other government agencies that maintain similar criminal databases, supporting the broader objectives of law enforcement agencies and the justice delivery system.

1.1 Project background

The Directorate of Forensic Science Services (DFSS) intends to establish the National Forensic Data Centre (NFDC) as a centralized repository for forensic data, designed to support law enforcement agencies and judicial authorities in criminal investigations, identification, prosecution, and the overall delivery of justice. This comprehensive database will include a wide range of forensic evidence/indices, such as DNA profiles, ballistic information, narcotics identification, questioned document analysis, and biometric data like facial and voice recognition.

By integrating these diverse forms of forensic indices, the NFDC will facilitate seamless information sharing across different jurisdictions, thereby enhancing the efficiency and effectiveness of crime-solving processes.

2. National Forensic Data Center (NFDC): Objectives

The key objectives and requirements of the National Forensic Data Center (NFDC) includes:

- **Establishing a State-of-the-Art National Database of Forensic Indices:** Creating an integrated platform that delivers next-generation forensic technologies and services.
- **Centralized Database Creation:** Developing a unified database encompassing DNA, ballistics, handwriting profiles, voice, face, and narcotic substance data for new enrolments, as well as for the search, matching, and verification of evidence/forensic indices.
- **Implementation of Infrastructure:** Deploying the necessary hardware, software, forensic equipment, and related services including seamless connectivity for accessing database for

the DFSS, existing seven (07) Central Forensic Science Laboratories (CFSLs) located across various states in India initially and later to be extended to more Central and State FSLs.

- **Data Hosting and Disaster Recovery Centre (DR):** Hosting data at the Data Centre (DC) which will be located at CFSL, Bhopal, with a Data Recovery (DR) site at Delhi/Hyderabad/ Pune (This will be decided based on the study which city is not prone to natural disaster), at a location to be communicated to the selected bidder. Maintain a fully synchronized Disaster Recovery Centre with the Data Centre, at CFSL, Bhopal ensuring continuous data replication and backup. The DR site should be capable of handling active loads in the event of Data Centre unavailability.
- **Centralized Forensic Data Archive Management System:** Establishing a robust system for storing critical forensic evidence/indices and reports, ensuring rapid accessibility and reference.
- **Comprehensive Support:** Providing continuous handholding and support for the National Forensic Database Centre at CFSL, Bhopal, for a period of five years, ensuring 24x7 availability through both online and offline modes.
- **Site Preparedness:** Ensure the installation of DG set and UPS systems for 24x7 power back up, firewalls, switches, network components, and provision of LAN connectivity at all designated locations. Configure workstations and supply furniture as per DFSS requirements.
- **Digitization of Physical Evidence and Records:** Digitize all existing evidence, records, documents, and related materials currently held by the seven (07) CFSLs to facilitate seamless integration into the centralized system.
- **Data Migration:** Transfer all digital data to the DFSS Data Centre at CFSL, Bhopal, establishing a unified and centralized forensic data repository from all the seven (07) CFSLs.
- **On-Premise Cloud Infrastructure:** Host, manage, and maintain forensic data and applications at the centralized Data Centre located at CFSL, Bhopal, utilizing on-premise cloud solutions.
- **Cyber Security Solutions for Data Protection:** Implement advanced cyber security measures to protect sensitive forensic information and criminal identities stored at the Data Centre. Utilize cutting-edge, trusted, and proven cyber security technologies.
- **Manpower Requirements:** Deploy trained and skilled personnel on a contractual basis at DC (CFSL, Bhopal) and the seven CFSLs to manage advanced forensic applications. Additionally, assign experienced staff to oversee the Central Data Centre and Disaster Recovery (DR) site, ensuring 24x7, year-round operations.
- **Training and Capacity Building:** Provide ongoing training and skill development for forensic scientists. Continuous training sessions in regular intervals should be conducted for scientific officers and staff in relevant forensic disciplines for the duration of the contract.
- **Network Connectivity:** Establish robust connectivity between DC, CFSLs, and the DR site using Multiprotocol Label Switching (MPLS) and Software-Defined Wide Area Network (SDWAN) technologies or any other advanced technologies, with failover devices at each location and adequate network bandwidth. Configure connectivity in a mesh (any-to-any) topology to ensure resilience and high availability.

3. Technical Requirements:

Please note that all the requirements mentioned in this section are the minimum and indicative in nature. The bidder must furnish Authorization Letter along with Certificate of compliance

from OEM or Algorithm Developer or both. Any authorization, certification or formation of consortium should be prior to the date of Last date of submission of Bid.

3.1 Accuracy

- The system should be capable of achieving accuracy not less than **99%** if the search is true match, then it should be in the first position **99%** of the time.
- The system should be capable of achieving accuracy for evidence search as; if the search is true match, then it should be in the first position **90%** of the time, in first three positions **95%** of the time and in top ten positions **99%** of the time.

3.2 Response Time

- Response time will be the time required for the server to search the evidences against the complete database and giving out the traced /untraced result and the search time should not exceed 1.0 second per search.
- The System should provide support the desired performance for 100 **CONCURRENT** user session on a high intensity matching workload. Separate price to be given for support.

3.3 Reporting and Dashboard

The output from the forensic systems must be user friendly and wherever matching needs to be displayed based on certain criteria as required by DFSS then such criteria should be configurable rather than hard coded.

System should guide Forensic Expert in manual verification so that Expert need not have to spend lot of time and quickly certify.

4. Forensic Solutions for NFDC

The NFDC shall have following core functions to implement the forensic solutions to enroll and identify the criminals using their forensic indices:

- Acquisition /Enrolment/Capture of Forensic Indices in the criminal cases
- Enabling Search/Query of forensic details from National Forensic Data Centre (NFDC)
- To interface with databases of other Forensic Indices for annotation of forensic details and reporting as required in the future to provide comprehensive criminal investigation.

The NFDC should have following forensic solutions and IT Infrastructure requirements:

Sl. No.	Forensic Applications with Database Sizing and IT Infra Solutions	Key objectives
1	**Criminal DNA Database Management System/software-** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL -** Minimum 1	The key objectives of Criminal DNA Database Management System/software includes the development, implementation, and maintenance of a secure and scalable centralized platform for storing, retrieving, and analyzing forensic DNA profiles. It involves integrating with DNA Extraction, Analysis

	million Profiles **At DC (CFSL, Bhopal) -** Minimum 15 million profiles	& DNA Profiling System in the lab, ensuring seamless data entry, automated matching, and compliance with legal and ethical standards. It should have Kinship analysis, suspect identification, and database cross-referencing for DNA profile search, match and verifications to correlate with the criminal's present and past crime records available in the NFDC.
2	**Automated Ballistics Examination System /software -** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL -** Minimum 50,000 Profiles **At DC (CFSL, Bhopal) -** Minimum 5,00,000 profiles	Automated Ballistics Examination System/software includes designing, implementing, and maintaining a centralized digital platform for analyzing and matching ballistic evidence. This includes integrating with advanced ballistic scanner for imaging, pattern recognition, and forensic database management to compare firearm markings on bullets and cartridge cases. It should have capabilities of 2D & 3D Visualization for scanned data of bullets, cartridges & their fragments. The ABES System should have identification, and database cross-referencing for fire arms profile search, match and verifications to correlate with the criminal's present and past crime records available in the NFDC.
3	**Handwriting Examination & Writer Identification System /software -** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL -** Minimum 50,000 Profiles **At DC (CFSL, Bhopal) -** Minimum 1 million profiles	Handwriting Examination & Writer Identification System/software involves the development and deployment of an advanced digital platform for analyzing, comparing, and identifying handwriting patterns and signatures in forensic examinations. This system must integrate AI-driven handwriting recognition, forensic document examination tools, and a centralized database of known handwriting samples. By connecting with remote Central Forensic Science Laboratories (CFSLs), it should enable real-time data sharing, automated comparison algorithms, and expert verification capabilities for forensic examination in document-related crimes.
4	**Video Examination & Face Recognition System /software -** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL** - Minimum 50,000 Profiles **At DC (CFSL, Bhopal) -** Minimum 1 million profiles	Video Examination & Face Recognition System/software involves the development and integration of an AI-powered platform for analyzing facial features and video evidence to aid forensic examinations. The system must incorporate advanced facial recognition algorithms, video enhancement tools, and a centralized database of known identities for real-time matching and suspect identification. By connecting with remote Central Forensic Science Laboratories (CFSLs), it should enable seamless data

		sharing, automated video analytics, and AI-driven forensic reconstruction, allowing experts to extract crucial evidence from surveillance footage, body cams, and other video sources.
5	**Audio Examination & Speaker Recognition System /software -** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL** - Minimum 50,000 Profiles **At DC (CFSL, Bhopal) -** Minimum 1 million profiles	Audio Examination & Speaker Recognition System/software involves the development and deployment of an AI-driven platform for analyzing and identifying speakers based on voice characteristics in forensic examinations. The system must integrate advanced voice biometrics, speech pattern analysis, and a centralized database of known voice samples for automated matching and suspect identification. By connecting with remote Central Forensic Science Laboratories (CFSLs), it should enable real-time data sharing, forensic audio enhancement, and AI-driven voice comparison, allowing experts to extract and analyze speech from recorded calls, surveillance audio, and digital evidence.
6	**Narcotic Substance Identification System /software -** Perpetual License with 5 years Service Support, Annual Trainings and software updates **At each CFSL** - Minimum 50,000 Profiles **At DC (CFSL, Bhopal) -** Minimum 1 million profiles	Narcotic Substance Identification System/software involves designing, developing and implementing a centralized digital platform for detecting, analyzing, and classifying narcotic substances in forensic examinations. The system must integrate with spectral analysis, chemical composition databases, and rapid drug detection system in lab to assist law enforcement in identifying illicit substances. By connecting with remote Central Forensic Science Laboratories (CFSLs), it should enable real-time data sharing, automated substance comparison, and remote expert verification, allowing forensic scientists to analyze seized drugs efficiently without physical evidence transfer.
7	**Forensic Data Management System /software -** Perpetual License with 5 years Service Support, Annual Trainings, software updates and customized Dashboards for centralized monitoring	The Forensic Data Management System//software involves the development and deployment of a secure, centralized platform for managing, analyzing, and archiving forensic evidence. The system must integrate AI-driven data analytics, digital evidence management, and advanced search capabilities to support forensic examinations. By connecting with remote Central Forensic Science Laboratories (CFSLs), it should enable real-time evidence tracking, automated case file management, and seamless data exchange, ensuring that forensic experts can access, analyze, and cross-reference evidence efficiently. This

		solution should be customized as per the requirements mentioned in this EOI and it should be integrated with all the mentioned forensic applications for evidence management in the lab and should provide required reports, analytics and dashboard for overall monitoring of the respective lab works. This solution shall be responsible to provide overall event-based analytics, reports and dashboard for data driven decisions to be taken by the CFSLs and DFSS. It should have provision to add additional Central and State Forensic Labs as and when required. It should integrate with Central Location DC (CFSL, BHOPAL) and will replicate the data on DR location only for Data DR Repository.
8	Dedicated Archival for Digital Evidence Management System for Storage and Analysis in Digital Forensics & IT Infrastructure and Cyber Security Solutions securing network connectivity at all the CFSLs and Data Centre (DC) & Disaster Recovery Centre (DR) **At each CFSL -** 1 PB Storage- Total 7PB at 7 CFSLs **At DC (CFSL, Bhopal) –** Initially 12PB (Scalable) for Central Archive for Critical Evidence Storage & Management **At DC (CFSL, Bhopal) -** Initially 12PB (Scalable) for Database & Storage requirements of Forensic Applications **At DR Site (Delhi/Hyderabad/Pune) -** Initially 12PB (Scalable) for Active-Passive DR Solution	**<u>Dedicated Archival for Digital Evidence Management System for Storage and Analysis in Digital Forensics</u> &** **<u>IT Infrastructure and Cyber Security Solutions</u>** • The solution should facilitate the process of collecting evidence from digital media sources and then segregate it to make it available for secured storage and analysis. • The system should streamline and secure the process of capturing sensitive documents, electronic data handling and compliance. • It should ensure swift access to critical information as well as provide a resilient and scalable infrastructure for hosting and accessing documents. • The entire process of the solution should involve ingestion, processing and development of a database that will store the entire evidence data segregated into the multiple data formats making it readily available for analysis. • The solution should control the accessibility of case documents at the CFSLs. • An interface should collate data from the mobile application, organize based on the required structure and feed the data lake with the evidence documents. Additionally, the interface will control role-based access for each user along with dedicated logs access. • Graphical representation of consolidated case related data permitting a user to analyze case patterns across segments such as demographics, regions, case types etc.

		• The dash boarding architecture should allow swift and user-controlled access to various cases within as well as across CFSLs. • To make data available on the central dashboard, a combined database of all the evidences of CFSLs should be created. These dashboards will be made available as analytics. The centralized dashboard will pick up incremental updates from the regional Evidence Database at CFSLs. • For each case, there should be a case ID, location and various evidences in different format. • Additionally, each CFSL location should be able to upload evidence data to central archival but can't fetch from there without permission from the authority • A chronological log to be maintained to record any form of access for a case or a document. To keep an effective control over processing of a document the chain of custody to additionally mention the action performed whilst accessing the document • Each record should have a timestamp to see when things happened. Also, people in the chain of custody have to report the access reason, which adds another level of responsibility. • The system generates a chain of custody document, detailing every person who handles the evidence, along with timestamps for each action • Digital signatures or authentication mechanisms should be used to ensure the integrity of the chain of custody of evidences. • All the forensic applications, IT Infrastructure and Cyber Security Solutions must be immediately updated with latest security patches/upgrades within 30 days of their release by the respective OEMs and the same shall be responsibility of the bidder to implement such updates/upgrades to meet the EOI requirements. **<u>At CFSLs</u>** • Each CFSL must operate independent processing units for all forensic applications and data, supporting real-time examinations with advanced analytics, security, audit trails, and regulatory compliance. • Evidence data from all CFSLs should be centrally archived, with permissions required for access and robust chain-of-custody tracking.

		<u>At DC (CFSL, Bhopal)</u> • DC would have all forensic processed data Server for search & matching of the data requests in Different Servers having VMs • Architecture would be based on scalable hardware and continuous upgradable software for all applications • Forensic Data Management System/software Solutions with Storage & Archive should be integrated with appropriate double module Usable Memory Architecture over Hardware Security Module (HSM) to manage the data flow and central repository for long term data preservation & data safety. • Archive storage should consider as unstructured data management without any compression as single replica • Forensic Data Management System/software application should able to replicate the entire database & archive data as it is to Disaster Recovery System (DR) system. • DC Should have Redundant Firewall and Core Switch Configuration • DC should have Central Network Management System (NMS) & Monitoring system to manage DC, All Branch location & DR. • DC should have single management console to manage Antivirus for all location • DC should have independent Back Manager software with required Backup storage for Infra backup replicated with DR Backup Manager • Forensic Data Management System/software Solutions should have API integration with All Forensic Application for Metadata level only to have National database search through a single Forensic Data Management System/software interface • Storage and Archive Management System should be integrated with Forensic Data Management System/software. • Hosts all processed forensic data with appropriate architecture redundancy and accessibility. • Integrates Forensic Data Management System/software with high-capacity storage on double module for long-term, uncompressed data preservation.

		• Supports full database and archive replication to Disaster Recovery (DR) systems. • Includes redundant firewalls, core switches, centralized monitoring, antivirus management, and backup solutions. • Forensic Data Management System/software provides API integration for metadata-level national database searches via a single interface. **<u>At DR Site (Delhi/Hyderabad/Pune)</u>** • Disaster Recovery Centre (DR Site) will be fully synchronized with Data Centre, at CFSL, Bhopal considering the data replication and Backup replication with only 10% active load considering the non-availability of DC. This will have an active-passive disaster recovery (DR) solution which features a primary site serving production traffic and a secondary site, also known as a standby site, that will be kept in synchronized and ready to take over if the primary site fails. The secondary site remains dormant until a failover event, offering cost savings and simplicity. • DR Energy Management System (EMS) Solutions with Storage & Archive should be integrated with appropriate double memory module Architecture over Hardware security modules (HSM) to manage the data flow integrated with DFSS EMS system • Archive storage should consider as unstructured data management without any compression as single replica • DC Should have Firewall and Core Switch Configuration • DR should have replicated Back Manager software from DC with Backup storage • Fully synchronized with DC (CFSL, Bhopal), maintaining replicated data and backups, handling 10% active load during DC outages. • Integrated with high-capacity storage and backup management, mirroring DC configurations for continuity.
9	Manpower requirements to Manage National Forensic Data Centre (NFDC) & Operations- 24x7 and 365 days service support	• Adequate trained manpower are to be deployed to manage the 24x7 and 365 days operation & service of the NFDC at all seven (07) CFSLs, DC and DR sites as per the approved DPR which will be discussed at

		the Prebid meeting with Database Sizing and IT Infra Solutions • This manpower requirement can be made flexible and changed according to the actual practical requirement once the functioning of the NFDC get started.

5. Important Notes for Bidders

The vendors may download EOI documents including this document containing technical details of the National Forensic Data Centre project from the DFSS website www.dfs.nic.in. If any clarifications are required, then such queries may be submitted to email-ID cfs-dfss@gov.in.

Standard terms and conditions of Government of India are applicable and detailed instructions for vendors are covered in this EOI. Accordingly, bidders may submit their EOI online as well as the hard copy in the sealed envelopes.

Before submission of EOI, vendors shall ensure that all the required information is furnished without any ambiguity and signed by authorized representative. Further, It is distinctly clarified that proposal must include all applicable taxes and missed items if any in this EOI for making the proposed solution operational.

DFSS's Right to terminate the Process

DFSS makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. Further, this EOI does not constitute an offer by DFSS. The vendor's participation in this process may result in DFSS selecting the bidder to engage in further discussions and negotiations towards execution of a contract.

6. Pre-Qualification Criteria

The bidder should meet the entire criterion mentioned below in order to qualify for the detailed bid evaluation i.e., Technical and Commercial evaluation.

Sl. No.	Qualification Criteria	Documentary Evidence
1.	**Though all reputed firm can participate in this EOI, preference is given to the participant/vendor who is a Central Government Public Sector Undertakings (PSU) company in India, registered under the Companies Act 1956 or 2013**	***A copy of certificate of registration under relevant act of India / relevant Country.***
2.	**Participant/vendor's quoting for this EOI must have at least 50 Cyber Forensic/Security or IT**	***Certificate from the HR head stating list of Employees with exposure to Projects and Technologies.***

	professionals working continuously full time for the past 1 year in India at the time of submission of bids.	***Name of the persons to be engaged for the project and their qualification and specialization also to be provided.*** ***If the employee discontinue/resigns from the position, the participant/vendor should deploy the substitute manpower within five (05) days.***
3.	**Participant/vendor's annual turnover should be at least Rs.400Cr. in each of the last 3 financial years.**	***Provide the copy of the audited financial statements of the company (bidder), and/or certificate from the Chartered Accountant***
4.	**Participant/vendor's should have a positive net worth in each of the last 3 financial years.**	***Provide copy of certificate from the Chartered Accountant specifying the net worth of the company***
5.	**Participant/vendor's should have supplied and implemented at least 2 Forensic Projects or established at least 2 Data Centre worth of 200Cr to any Central or State Govt. entity in India in last 5 financial years or should have similar global implementation experiences with Govt. agencies.**	***Copy of client citations / Work Orders for AFIS installations OR client letter / testimonial stating the completion of the project and working satisfactorily in operations phase.*** ***Reference for each of the projects has to be given and should contain the following information - Name of organization, individual/s to contact, email-id, phone number and address, contract value and project details***
6.	**Participant/vendor's should have valid documentary proof of Sales tax/GST registration number**	***Provide copy of Sales Tax/GST registration number***
7.	**Participant/vendor's should have Certificate of Incorporation (CIN) and PAN card**	***Provide copy of required certificates***
8.	**Participant/vendor's should not have been blacklisted by Central government, State governments or government corporations of India as on the date of bid submission.**	***Undertaking/self-declaration and should be submitted along with the technical bid.***
9.	**Demonstration/Presentation of application at the time of evaluation**	***The Participant/vendor must demonstrate or present their offered product at onsite decided by the DFSS, Hqtr.***

7. Bidding and Evaluation

7.1 Bid opening sessions

- Total transparency will be observed while opening the proposals/bids.
- DFSS/MHA, reserves the rights at all times to postpone or cancel a scheduled bid opening.

- During bid opening preliminary scrutiny of the bid documents will be made to determine whether they are complete, whether required bid security has been furnished, whether the documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements will be prima facie rejected.

7.2 Technical Proposal

- Technical proposal should include all the mandatory undertakings
- The technical proposal should address all the areas/ sections as specified by the EOI and should contain a detailed description of how the bidder will provide the required services outlined in this EOI. It should articulate in detail, as to how the bidder's Technical Solution meets the requirements specified in the EOI.
- The technical proposal should outline the proposed methodology for
    a) Change Management / Capacity building, and
    b) Exit management
- The Technical Proposal should be structured under the following minimum heads:
    a) Overview of the proposed solution that meets the requirements specified in the EOI
    b) Details of the Solution as per the format provided in the EOI
    c) Overall proposed Solution, technology, and deployment architecture
    d) Security architecture
    e) Integration and Interfacing Architecture
    f) Bill of material of all the components (i.e. software, hardware, etc.) as per the formats provided in the EOI
    g) Approach & methodology for project development and implementation including the project plan
    h) Overall Governance Structure and Escalation Mechanism
    i) Project team structure, size, capability and deployment plan (Total Staffing plan including numbers)
    j) Training and Communication Strategy for key stakeholders of the project
    k) Key Deliverables (along with example deliverables, where possible)
    l) Project Management, reporting and review methodology
    m) Strategy for conducting Operations & Maintenance
    n) Risk Management approach and plan
    o) Certification from the OEMs on the Infrastructure proposed by bidder
    p) Bidder's experience in all the project related areas as highlighted in Bid evaluation criteria