

Request for Expression of Interest (EoI)

For

Network Upgradation and Internet Services at
CIET-NCERT

Central Institute of Educational Technology,
National Council of Educational Research & Training,
Sri Aurobindo Marg,
New Delhi- 110016

1. Introduction

CIET, a constituent unit of NCERT, is engaged in development and dissemination of digital educational resources, online learning systems, educational broadcasting, multimedia production, and ICT-enabled academic activities. The institute requires a modern, secure, scalable, and centrally managed network infrastructure to support its expanding digital ecosystem and uninterrupted operations.

The existing infrastructure requires comprehensive modernization to support:

- High-speed internet connectivity
- Centralized wired and wireless networking
- Secure access management
- Advanced cybersecurity mechanisms
- Redundant internet architecture
- Unified monitoring and management
- Seamless connectivity for staffs, studios and all technical areas.
- Future scalability for emerging technologies and digital services

Accordingly, CIET intends to undertake upgradation of its complete internet and network infrastructure.

Also, Since CIET and NCERT are functioning from co-sited premises, the proposed Internet and Network Architecture under the EoI should be designed with interoperability and compatibility with the existing NCERT network infrastructure. The proposed architecture should support seamless interconnectivity, redundancy, and failover integration between CIET and NCERT networks so that, in the event of failure or disruption of any internet/network service at either end, connectivity and critical network services may continue through the available infrastructure of the other organization with minimum downtime and operational interruption.

2. Objective Of The EoI

The objective of this EoI is to invite proposals from eligible agencies for:

- Upgradation of Core Network Infrastructure
- Modernization of LAN Infrastructure
- Enterprise-grade Wi-Fi deployment
- Advanced Firewall and Network Security implementation
- Internet Redundancy and Load Balancing
- Centralized Network Monitoring & Management
- Secure User Authentication & Access Control
- Network Segmentation and Policy Enforcement
- Scalable and future-ready network architecture
- High availability and uninterrupted network operations

3. Scope Of Work

The Expression of Interest (EoI) is intended to invite responses, technical approaches, conceptual solutions, architecture recommendations, capability details, and indicative methodologies from reputed agencies/vendors having expertise in enterprise-grade internet and network infrastructure solutions. The broad areas for which inputs are invited include the following:

3.1 Core Network Infrastructure

- Design and deployment of enterprise-grade core switching architecture.
- High-speed backbone connectivity.
- Redundant core network design.
- VLAN and network segmentation.
- Layer-3 routing and traffic optimization.
- Integration with existing infrastructure.
- Support for IPv4/IPv6.
- Centralized network control and management

3.2 LAN Infrastructure

- Upgradation of existing LAN infrastructure.
- Managed Gigabit/10G access switches.
- Structured cabling integration.
- PoE-enabled switching infrastructure.
- High-speed connectivity for offices, studios, labs, classrooms, and conference areas.
- Redundant uplink architecture.
- Rack integration and cable management.

3.3 Wi-Fi Infrastructure

- Deployment of centrally managed enterprise Wi-Fi solution.
- Wi-Fi coverage for office areas, conference rooms, studios, labs, other technical areas and common areas.
- Seamless roaming and centralized SSID management.
- Support for latest Wi-Fi standards.
- Guest access management.
- User authentication and role-based access.
- Traffic analytics and monitoring.
- High-density user support.

3.4 Firewall & Security Infrastructure

- Deployment of enterprise-grade Next Generation Firewall (NGFW)/Unified Threat Management (UTM).
- Intrusion Prevention System (IPS).
- Intrusion Detection System (IDS).
- Antivirus, Anti-malware, and Web Filtering.
- Application visibility and control.
- VPN support for remote access.

- Network Access Control (NAC).
- Security policy enforcement.
- Content filtering and bandwidth management.
- SSL inspection and threat intelligence.
- Security logging and reporting.

3.5 Internet Architecture & Redundancy

- Integration of multiple internet service providers.
- Intelligent failover and redundancy.
- Load balancing.
- Bandwidth optimization.
- Redundant internet gateway architecture.
- NKN integration compatibility.
- High availability network design.

3.6 Monitoring & Management System

- Centralized network management platform.
- Real-time monitoring of devices and bandwidth.
- Dashboard-based monitoring.
- Event logging and alerting.
- User activity monitoring.
- Device health monitoring.
- Historical reporting and analytics.
- Configuration backup and restoration.

3.7 Implementation & Support

- Site survey and requirement assessment.
- Network design and architecture planning.
- Supply and installation of all required equipment.
- Configuration, integration, testing, and commissioning.
- Documentation and as-built drawings.
- Training for technical personnel.
- Warranty and post-installation support.

3.8 Integration with Existing NCERT Network Infrastructure

Since CIET and NCERT are functioning from co-sited premises, the proposed Internet and Network Architecture shall be designed in a manner that ensures seamless interoperability and compatibility with the existing NCERT network infrastructure.

The proposed solution should ensure minimal disruption to existing services during implementation and migration activities. The architecture should also provide flexibility for future upgrades, centralized monitoring, and integration with additional institutional or government network ecosystems.

4. Response Expectations

Interested agency/vendors may do a field survey of CIET and provide:

- Conceptual architecture approach.
- Recommended network modernization strategy.
- Proposed internet architecture framework.
- Approach for secure and scalable infrastructure.
- Suggestions for redundancy and high availability.
- Proposed cybersecurity framework.
- Recommendations for centralized monitoring and management.
- Scalability considerations for future expansion.
- Relevant experience and case studies.
- Indicative implementation methodology.
- OEM ecosystem and technology stack.
- Proposed approach and timeline for executing the project.
- The proposed components/equipment, tentative quantities, and indicative budgetary pricing for the proposed Internet and Network Architecture solution

5. Eligibility Criteria

The interested agencies/vendors should fulfil the following criteria:

1. The agency should be a registered company/firm in India.
2. The agency should have experience in planning, installation, maintenance and implementation of internet networking projects in Govt./Abs/PSUs etc.
3. The agency should have experience of at least 03 years in deployment of integrated LAN/Wi-Fi/Security infrastructure.
4. The agency should have technical manpower with relevant certifications.
5. The agency should not be blacklisted by any Government organization/PSU/ABs.

6. Documents To Be Submitted

Interested agencies/vendors shall submit:

- Company profile.
- Certificate of incorporation/registration.
- PAN & GST registration.
- Relevant experience details of similar projects.
- Technical certifications and competencies.
- OEM partnerships/authorizations, if any.
- Declaration regarding non-blacklisting.

7. Future Scalability Requirement

The proposed architecture should be scalable and capable of supporting:

- Future bandwidth expansion.
- Additional access points and network devices.
- Expansion of user base.

- Additional security layers.
- Smart classroom and digital studio integration.
- AV conferencing systems.
- Cloud and hybrid services.
- Centralized authentication systems.
- Advanced analytics and monitoring tools.

8. General Terms & Conditions

1. This EoI is issued solely for obtaining information, technical inputs, and understanding available technologies and solution approaches in the market.
2. This document is not a tender/RFP and does not constitute any commitment for procurement or award of work.
3. Participation in this EoI process shall not entitle any organization to claim any right for empanelment, award, or commercial engagement.
4. CIET reserves the right to accept, reject, or modify the EoI process without assigning any reason.
5. The information received through this EoI may be utilized for preparation of future technical requirements, tender documents, or procurement strategies.
6. The agency shall ensure interoperability and compatibility of all proposed components.
7. All products proposed should be genuine, new, and from reputed OEMs.
8. All proposed equipment should ensure compliance with applicable cybersecurity and IT standards.
9. Interested agencies are advised to conduct detailed site survey before submission of EoI response.
10. The proposed solution should comply with prevailing Government of India cyber security guidelines, CERT-In advisories and standard logging/audit requirements applicable to institutional network infrastructure.
11. Information shared during site survey/discussions shall be treated as confidential and shall not be disclosed without prior approval of CIET.

9. Timeline

- a) EOI Release Date: 15th July, 2026
- b) Date & Time of Site Survey at CIET: 22nd July, 2026 at 10:00 A.M.
- c) EOI Submission Deadline: 30th July, 2026

10. Clarification & Query

Interested agencies/vendors may submit their queries, if any, through e-mail at ciet.networking@ciet.nic.in on or before 24th July 2026.

All queries received within the stipulated time shall be consolidated, and a common response/clarification shall be issued on the following day for the information of all.