National Law University and Judicial Academy, Assam

(Established by Assam Act No. XXV of 2009)

No. NLUJAA/ADMIN/F/IT-AUDIT/2026/42/ 606 Date: 26.06.2026

SHORT NOTICE INVITING QUOTATION (SNIQ)

FOR

COMPREHENSIVE INFORMATION TECHNOLOGY (IT), INFORMATION SECURITY, CYBER SECURITY, NETWORK, DIGITAL ASSET, WEBSITE, EMAIL, ERP AND CCTV INFRASTRUCTURE AUDIT OF NATIONAL LAW UNIVERSITY AND JUDICIAL ACADEMY, ASSAM (NLUJAA)

Sealed quotations, affixed with non-refundable Court Fee Stamps of Rs. 8.25/- (Rupees Eight and Twenty Five paisa) or as applicable in concerned state only, are hereby invited from reputed firms/contractor/bidders/individuals for comprehensive Information Technology (IT), Information Security, Cyber Security, Network, Digital Asset, Website, Email, ERP and CCTV infrastructure audit of national law university and judicial academy, assam (NLUJAA) as per the details and terms & conditions given below, which will be received at the office of the Registrar, NLUJA, Assam during office hours up to **01:30 PM** on or before **02-07-2026 and will be opened on the same day at 02:00 PM.** The Quotationers/Tenderers or their authorized agents may remain present at the time of opening of the quotations.

1. INTRODUCTION

National Law University and Judicial Academy, Assam (NLUJAA) invites sealed quotations under a Two-Bid System (Technical Bid and Financial Bid) from reputed firms having demonstrable expertise in Information Systems Audit, Information Security Audit, Cyber Security Assessment, Network Audit, Vulnerability Assessment and Penetration Testing (VAPT), IT Governance and Digital Infrastructure Review for undertaking a comprehensive audit of the University's Information Technology ecosystem.

The objective of the audit is to assess the adequacy, effectiveness, security, compliance, resilience, utilization and governance of all information technology resources and systems deployed by the University and to identify risks, vulnerabilities and opportunities for improvement.

2. SCOPE OF WORK

The audit shall be enterprise-wide and shall include all campuses, offices, departments, centres, laboratories, hostels, libraries and other units of the University.

The scope shall include, but not be limited to, the following:

A. IT ASSET AUDIT

Physical verification, validation and reconciliation of all IT assets, including:

- Desktop Computers (230 nos. approx.)
- Laptops (10 nos. approx.)
- Workstations
- Servers (12 nos. approx.)
- Storage Devices
- Printers and Multifunction Devices (50 nos. approx.)
- Projectors (25 nos. approx.)
- Smart Classroom Infrastructure (14 nos. approx.)
- Biometric Attendance Systems (4 nos. approx.)
- UPS Systems connected to IT infrastructure (8 nos. approx.)
- Wi-Fi Controllers and Access Points (60 nos. approx.)
- CCTV Infrastructure (170 Nos. approx.)

The auditor shall:

i. Verify physical existence of assets.

ii. Reconcile assets with institutional records.

iii. Verify asset tagging and inventory management systems.

iv. Identify obsolete, redundant, unsupported and non-functional assets.

v. Assess warranty, AMC and support status.

B. NETWORK INFRASTRUCTURE AUDIT

Assessment of:

- Core Network Architecture
- Routers
- Switches
- Firewalls
- Wireless Networks
- Internet Leased Lines
- VPN Infrastructure
- VLAN Configuration
- Network Segmentation
- Redundancy and Failover Mechanisms

The audit shall include:

i. Network topology mapping.

ii. Review of bandwidth utilization.

iii. Review of network security controls.

iv. Identification of single points of failure.

v. Recommendations for optimization and security enhancement.

C. INFORMATION SECURITY AND CYBER SECURITY AUDIT

Assessment of the University's overall cyber security posture.

The audit shall include:

i. Vulnerability Assessment of systems and devices.
ii. Security configuration review.
iii. User privilege review.
iv. Endpoint security assessment.
v. Antivirus and Endpoint Detection and Response (EDR) review.
vi. Patch management review.
vii. Security monitoring mechanisms.
viii. Malware protection measures.
ix. Security incident response preparedness.
x. Risk assessment and threat exposure analysis.

D. EMAIL INFRASTRUCTURE AND COMMUNICATION SYSTEM AUDIT

Assessment of all institutional email systems and communication platforms.

The audit shall examine:

i. Email server architecture and administration.
ii. User account provisioning and de-provisioning.
iii. Shared mailboxes.
iv. Mail forwarding rules.
v. Email retention policies.
vi. Email archival mechanisms.
vii. Access logs and audit trails.
viii. Administrative privileges.
ix. Authentication controls including MFA, SPF, DKIM and DMARC.
x. Detection and prevention of unauthorized access.
xi. Security of official communications.
xii. Historical logging and traceability mechanisms.

E. IDENTITY AND ACCESS MANAGEMENT (IAM) AUDIT

Review of:

i. User account lifecycle management.
ii. Dormant accounts.
iii. Former employee accounts.
iv. Administrative and privileged accounts.
v. Role-based access controls.
vi. Segregation of duties.
vii. Password policies.
viii. Multi-factor authentication implementation.
ix. User access review mechanisms.

F. SERVER, DATA CENTRE AND CLOUD INFRASTRUCTURE AUDIT

Assessment of:

i. Physical server infrastructure.
ii. Virtualized environments.
iii. Cloud-based infrastructure.
iv. Backup systems.
v. Disaster Recovery arrangements.
vi. Data storage and protection mechanisms.
vii. Data Centre physical security.
viii. Environmental controls.
ix. Server utilization and performance.

G. ERP, ACADEMIC AND ADMINISTRATIVE SYSTEMS AUDIT

Assessment of all institutional software systems, including:

- Academic ERP
- Student Information Systems
- Admission Management Systems
- Examination Management Systems
- Finance and Accounts Software
- Payroll Systems
- Human Resource Systems

- Library Management Systems
- Digital Repository Systems

The audit shall verify:

i. Data integrity.
ii. User privileges.
iii. Segregation of duties.
iv. Transaction controls.
v. Audit trails.
vi. System security.
vii. Backup and recovery arrangements.

H. WEBSITE AND WEB APPLICATION SECURITY AUDIT

The auditor shall conduct:

i. Website security review.
ii. Vulnerability Assessment and Penetration Testing (VAPT).
iii. OWASP Top-10 vulnerability assessment.
iv. Authentication and authorization review.
v. SSL/TLS configuration review.
vi. Database security review.
vii. Hosting infrastructure review.
viii. Third-party integration review.

I. CCTV AND ELECTRONIC SURVEILLANCE AUDIT

Comprehensive assessment of:

- CCTV Cameras
- NVR/DVR Systems
- Recording Infrastructure
- Storage Systems
- Monitoring Facilities

The audit shall include:

i. Physical verification.
ii. Coverage adequacy assessment.

iii. Identification of blind spots.
iv. Camera functionality assessment.
v. Recording retention review.
vi. Storage utilization review.
vii. Security of surveillance systems.
viii. Access control over recorded footage.
ix. Network security of CCTV infrastructure.
x. Recommendations for enhanced surveillance coverage.

J. SOFTWARE LICENSE AND COMPLIANCE AUDIT

Assessment of:

i. Licensed software inventory.
ii. Unauthorized software installations.
iii. License compliance.
iv. Vendor support status.
v. Open-source software risks.

K. DATA PROTECTION, PRIVACY AND REGULATORY COMPLIANCE REVIEW

Assessment of institutional preparedness with reference to:

- Digital Personal Data Protection Act, 2023
- CERT-In Directions
- Relevant Government of India Cyber Security Advisories
- Applicable UGC Guidelines

The review shall include:

i. Personal data repositories.
ii. Sensitive data management.
iii. Data retention practices.
iv. Data sharing practices.
v. Data governance mechanisms.

L. DISASTER RECOVERY AND BUSINESS CONTINUITY AUDIT

Assessment of:

i. Backup policies.
ii. Backup restoration testing.
iii. Disaster Recovery Plans.
iv. Business Continuity Plans.

M. DIGITAL FORENSICS READINESS ASSESSMENT

The auditor shall assess:

i. System logging mechanisms.
ii. Log retention policies.
iii. Log integrity controls.
iv. Time synchronization mechanisms.
v. Incident response preparedness.
vi. Evidence preservation capability.
vii. Capability to investigate unauthorized access incidents.

N. PHYSICAL SECURITY REVIEW OF IT INFRASTRUCTURE

Assessment of:

i. Server room security.
ii. Access controls.
iii. Visitor management systems.
iv. Key management.
v. Environmental safeguards.
vi. Fire detection and suppression systems.
vii. Power backup arrangements.

O. IT GOVERNANCE REVIEW

Assessment of:

- IT Policies
- Cyber Security Policies
- Access Control Policies
- Backup Policies
- Incident Response Policies
- Asset Management Procedures
- Business Continuity Policies

The auditor shall identify policy gaps and recommend improvements.

3. SPECIAL CERTIFICATION REQUIREMENT

The selected agency shall specifically certify whether any system architecture, administrative privilege assignment, access control mechanism, email configuration, logging configuration, network design, software implementation or operational practice creates a possibility of unauthorized access to:

- Official communications
- Institutional email accounts
- Electronic records
- Databases
- CCTV recordings
- User accounts
- Confidential institutional information

and recommend corrective measures.

4. DELIVERABLES

The agency shall submit:

i. Asset Verification Report.

ii. Network Infrastructure Audit Report.

iii. Information Security Assessment Report.

iv. Email Infrastructure Audit Report.

v. ERP and Application Audit Report.

vi. CCTV Audit Report.

vii. Vulnerability Assessment and Penetration Testing Report.

viii. Compliance Gap Analysis Report.

ix. Digital Forensics Readiness Assessment Report.

x. Risk Register.

xi. Network Topology Diagram.

xii. CCTV Coverage Assessment Map.

xiii. Executive Summary Report.

xiv. Comprehensive Final Audit Report.

xv. Prioritized Remediation Roadmap.

xvi. Presentation before University Authorities.

5. ELIGIBILITY CRITERIA

The bidder shall:
a) Be a Company, LLP or Partnership Firm legally registered in India.
b) Have minimum five years' experience in Information Systems Audit/Cyber Security Audit.
c) Have completed at least three similar assignments for Universities, Government Departments, PSUs, Regulatory Bodies, Autonomous Institutions or Banking Institutions during the preceding five years.
d) Possess an average annual turnover of not less than Rs. 25 Lakhs during the last three financial years.
e) Have qualified professionals possessing one or more of the following certifications:

- CISA
- CISSP
- CISM
- CEH
- ISO 27001 Lead Auditor
- ISO 22301 Lead Auditor
- OSCP (Desirable)

f) Not have been blacklisted by any Government Department, PSU, University or Statutory Authority.

6. TWO-BID SYSTEM

A. TECHNICAL BID

The Technical Bid shall contain:

i. Firm Profile
ii. Registration Documents
iii. PAN and GST Registration
iv. Audited Financial Statements for last three years
v. Experience Certificates and Work Orders
vi. Team Composition and CVs
vii. Professional Certifications
viii. Methodology and Audit Plan
ix. Project Schedule
x. Non-Blacklisting Declaration
xi. Court Fee Stamps Rs. 8.25/- or as applicable in concerned state only
xii. Tender Fee **Rs. 1000/-** (in the form of Demand Draft drawn on any Nationalised/Scheduled bank in India in favour of "Registrar, National Law University and Judicial Academy, Assam" payable at Guwahati as EMD)
xiii. EMD of **Rs. 25,000/-** (in the form of Demand Draft drawn on any Nationalised/Scheduled bank in India in favour of "Registrar, National Law University and Judicial Academy, Assam" payable at Guwahati as EMD)

No financial information shall be included in the Technical Bid.

B. FINANCIAL BID (to be submitted in the separated sealed envelope)

Sl. No.	Component	Amount (Rs.)	Remarks
1	IT Asset Audit		
2	Network Audit		
3	Information Security Audit		
4	Email Infrastructure Audit		
5	ERP and Application Audit		
6	Website Security Audit and VAPT		
7	CCTV Audit		
8	Compliance and Governance Review		
9	Digital Forensics Readiness Assessment		
10	Reporting and Presentation		
11	**Total Professional Fee**		
12	**GST (if applicable)**		
13	**Grand Total in Rs.**		

The quoted amount shall be inclusive of all travel, boarding, lodging, manpower, software tools, testing utilities and incidental expenses.

7. TIMELINE

The assignment shall be completed within forty-five (45) days from the date of issuance of the Work Order.

8. CONFIDENTIALITY

The selected agency shall execute a Non-Disclosure Agreement (NDA) and maintain strict confidentiality regarding all information, systems, records, credentials, logs and data accessed during the course of the audit.

9. RIGHTS OF THE UNIVERSITY

The University reserves the right to accept or reject any or all quotations, wholly or partly, without assigning any reason whatsoever and shall not be bound to accept the lowest quotation.

10. General Terms and Conditions:

1. The rates should be quoted as shown against the items/articles and should be inclusive of GST/taxes applicable at any point of time.
2. The sealed envelope should bear the following 'superscription' on the top:
   "The Registrar, National Law University and Judicial Academy, Assam".
3. The undersigned reserves the right to accept or reject any tender without assigning any reason thereof.
4. Any deviation from terms and conditions shall invite cancellation of Quotation/Tender/Bills etc. and forfeiture of security deposit.
5. Bills must be submitted within 07 (seven) days of work completion, along with work order for payment.
6. Any firm/supplier indulging in any malpractice or adopting any unfair means will be barred from working with the University.
7. Past records of the firms/suppliers/contractors will be duly considered while awarding the work.
8. Screening procedure may factor in other conditions deemed to be just, fit and proper at that point of time.

Registrar
NLUJA, Assam

Memo No. NLUJAA/ADMIN/F/IT-AUDIT/2026/42/ 607-610 Date: 26.06.2026

Copy to:

1. System Administrator with a request to upload in the University website.
2. P.S. to VC for kind appraisal of the Hon'ble Vice-Chancellor
3. Notice Board
4. Office File

Registrar
NLUJA, Assam