Government of India

Ministry of Electronics and Information Technology

*****

NOTICE

Subject: "Call for Proposals" for Establishing Centres of Excellence for Policy, Law and Technical Research in Cyber Space – reg.

The Ministry of Electronics and Information Technology (MeitY) invites proposal for establishment of Centres of Excellence for policy, law and technical research in cyber space.

The guidelines for submission of proposal indicating objectives, financing, proforma of application etc. are placed with this notice.

The last date of submission of application is 22nd April, 2026.

The proposal shall be submitted through email coe-cyberlaws@meity.gov.in .

Call for Proposals for Establishing Centres of Excellence for Policy, Law and Technical Research in Cyber Space

I. Background

The rapid evolution of the digital ecosystem has introduced complex challenges requiring integrated legal, policy, and technical responses. Dedicated centres for policy, law, and technical research in cyberspace are essential to strengthen India's cyber law and digital governance framework by bridging research, policymaking, and implementation. These centres will serve as institutional anchors to enhance national cyber security & resilience and support secure, inclusive, and sustainable digital development.

To establish Centres of Excellence (CoEs) that position India as a global leader in cyber law, policy, and digital governance through evidence and knowledge-based research, secure and scalable technical solutions, and interdisciplinary collaboration. The CoEs will strengthen national cyber resilience, safeguard digital rights, and reinforce India's digital sovereignty amid rapid technological change.

The CoEs are envisioned to:

1. **Advance Evidence-Based Cyber Law and Policy Development**

   To serve as premier research institutions generating rigorous legal and policy research that informs the development, reform, and refinement of the nation's regulatory framework for cyberspace, digital governance, and emerging technologies.

2. **Bridge Technology and Legal Compliance**

   To develop innovative technological solutions that facilitate effective implementation of cyber laws, enhance regulatory compliance mechanisms, and address enforcement challenges in the rapidly evolving digital ecosystem.

3. **Build National Capacity and Expertise**

   To cultivate specialized interdisciplinary expertise in cyber law, digital policy, and technology governance through advanced research, training initiatives, and knowledge networks that strengthen India's institutional capacity.

4. **Foster Digital Resilience and Rights-Based Frameworks**

   To design holistic governance frameworks that reconcile competing interests and values in the digital ecosystem, ensuring human-centric, adaptive, and sustainable digital governance that upholds fundamental rights while enabling technological progress and societal benefit.

5. **Provide Strategic Foresight on Emerging Technologies**

   To systematically monitor, analyse, and assess legal, ethical, and societal implications of emerging technologies, and provide proactive policy guidance that enables responsible innovation and ensures policy frameworks evolve in step with technological advancement.

II. Scope of Work

A. Legal and Policy Research

1. Research and Analysis of Digital Governance Frameworks

Conduct research on cyber laws, evolving digital governance frameworks, and emerging regulatory issues. Outputs may include comparative analyses, white papers and policy briefs, regulatory impact assessments, and gap analyses to identify areas for intervention.

2. Stakeholder Consultation and Participatory Research

Design and facilitate multi-stakeholder consultations, expert roundtables, and deliberative forums on key cyber policy issues. Undertake interdisciplinary and cross-sectoral research through participatory processes involving government, industry, academia, and civil society.

3. Implementation Support and Guidance

Develop implementation frameworks, operational guidelines, and compliance toolkits for cyber laws and policies, including legal and technical support to government agencies during policy rollout and enforcement design.

4. Frontier Research and Risk Assessment

Study emerging technologies, associated societal risks, and policy challenges arising from the evolving digital ecosystem. Undertake forward-looking research to assess

implications and provide actionable governance foresight to support proactive regulatory frameworks.

B. Technical Research and Development

1. Compliance Technology and Implementation Tools

Develop technological solutions to support effective implementation of cyber laws and regulatory compliance, including compliance workflows, reporting and audit mechanisms, privacy-by-design frameworks, and enforcement support tools.

2. Technology-Policy Interface Research

Conduct technical research at the technology–policy interface to inform evidence-based governance frameworks, including technical assessments of regulatory proposals, evaluation of policy effectiveness, and development of guidelines for secure digital infrastructure.

3. Addressing Emerging Threats and Technologies

Undertake technical research on emerging technologies and digital risks to generate actionable insights, prototype solutions, and practical guidance that strengthen cyber law implementation and support timely, informed governance responses.

C. Capacity Building and Knowledge Dissemination

1. Professional Development and Institutional Capacity

Design and implement specialized training programmes for the judiciary, law enforcement, policymakers, and government officials on cyber law and technology governance through workshops, seminars, and learning modules to build interdisciplinary expertise and institutional capacity.

2. Knowledge Development and Dissemination

Develop and disseminate educational resources on digital rights, online safety, and cyber governance to enhance digital literacy and public awareness. Publish research outputs, including policy briefs, working papers, and analytical reports.

IV. Education and Talent Development

1. Specialized Expertise Development

Cultivate specialized expertise in cyber law, digital policy, and technology governance through advanced training programmes, specialized courses, and continuous professional development initiatives.

2. Talent Cultivation

Develop a pipeline of interdisciplinary experts to address complex challenges at the intersection of law, policy, and technology through targeted education and research opportunities.

III. Institutional Framework and Partnership Model

Institutional Framework

- Recognizing that robust cyber law and policy research requires both deep legal expertise and technical implementation capabilities, the CoE(s) shall operate under a multi-institution collaborative model comprising a Lead Institution which shall be a recognised and accredited law department or university and one or more Technical Partner(s) which shall be a recognised and accredited technical institutions.

- Up to three (3) applicants may be selected pursuant to this call for proposals to establish the CoE(s) while ensuring regional diversity.

Roles and Responsibilities

- The Lead Institution shall be responsible for overall project management, coordination with the Ministry of Electronics and Information Technology (MeitY), and delivery of all final outputs, serving as the administrative and financial anchor for the Centre.
- The Technical Partner shall provide specialized technical expertise, infrastructure, and implementation support, working collaboratively with the Lead Institution.

Collaborative Engagement and Specialized Partnerships

To fulfil its multifaceted objectives, the CoE(s) will have the flexibility to hire or onboard specialized organizations or subject matter experts with domain expertise in tech-policy, law and technology, cybersecurity, data protection, or other relevant areas.

IV. Nature and Duration of funding

Funding Structure

Each CoE will be supported with a funding of upto ₹30 crore for five years as grant for establishing and operating the CoE(s), with funding disbursed on an annual basis against predetermined objectives, deliverables, and performance milestones. Funding will cover human resources, essential equipment, data acquisition, software licences, analytical tools, capacity building activities, consumables, travel, contingency, and overheads. MeitY shall sanction a five-year grant to the Lead Institution(s) for establishing and operating the CoE(s), with funding disbursed on an annual basis against predetermined objectives, deliverables, and performance milestones.

Mode of Funding

- Funding will be released directly to the Lead Institution with which the Principal Investigator and Co-Investigator(s) are affiliated.
- Disbursement will be made on an annual basis, aligned with approved project deliverables and the item-wise cost breakdown.
- The Lead Institution shall be responsible for further disbursing funds to the technical partner(s) and any other collaborating organisations, in accordance with the approved budget and partnership arrangements.

Financial Sustainability and Revenue Generation

- During the five-year grant period, the CoE(s) may generate supplementary funding through independent policy research and consultancy for government and non-government organisations. Supplementary funding from any State instrumentality shall be availed upon notifying MeitY, and funding from non-government organisations shall require prior written approval from MeitY.

- Beyond the five-year grant from MeitY, the CoE(s) shall operate on a fully self-sustaining basis through diversified revenue streams to ensure long-term viability.

V. Eligibility Criteria

- Applications are invited from recognised and accredited law universities or law departments within a recognised and accredited university with a proven track record in legal and policy research, applying in partnership with recognised and accredited technical institution(s) possessing strong capabilities in innovation, engineering, and implementation.

- The lead applicant must have a letter of intent with the technical partner(s) for the purpose of establishing the CoE(s).
- Upon selection of the proposal, the lead applicant must, within a three month timeframe, establish a specific MoU with the technical partner(s) for collaboration on the Centre. In the event of a pre-existing MoU or agreement between the applicant and technical partner(s), collaboration on this CoE(s) must be specifically identified under such agreement.

S.No.	**Minimum Eligibility Criteria**	**Demonstration of Requirement**
1.	**Institutional Qualification** Applicant may be: ● Central/ State Government Law Universities ● Law Department within other Universities, accredited under the UGC framework. Applicant must offer: ● Undergraduate and post-graduate programs in law, and ● Study of cyber-laws as part of the curriculum of both Undergraduate and post-graduate.	Relevant accreditation certificates under the UGC framework
2.	**Technical Partner(s) Information** Technical Partner(s) must be: • Recognised and accredited technical institutions (engineering, computer science, or technology-focused institutions) • Institutions with proven capabilities in innovation, engineering, and technical implementation	• Relevant accreditation certificates under the UGC framework • Letter of Intent from Technical Partner(s) for collaboration on the Centre
4.	**Applicant's Profile**	Citizenship proof,

	The Principal Investigator and Co-Investigator(s) must be Indian citizens. The Principal Investigator must hold regular full-time academic or faculty position at the University or Law Department. The Co-Investigator(s) must hold regular full-time positions at the University or Law Department or Technical Partner Institution.	employment letter from the institution

VI. Evaluation Framework and Selection Process

S.No.	Parameter	Sub-criteria		Maximum Marks
1.	**Lead Institution Profile**	**Academic standing, ranking, and accreditations**	The applicant (lead) institution must demonstrate strong and consistent academic standing over the last three years, evidenced through international collaborations, rankings or accreditations such as the National Institutional Ranking Framework (NIRF) of the Ministry of Education.	10
		Prior Research in Cyber Law / Technology Policy	Demonstrated record of publications, policy papers, or projects in domains such as cyber law, artificial intelligence,	15

			digital governance, or data protection.	
		Research Infrastructure and Capacity	Availability of advanced research infrastructure and capacity to host multidisciplinary research teams in law, policy, and technology domains.	10
		Past Government Collaboration	Evidence of prior collaboration with government on developing laws, policy frameworks, or capacity-building initiatives for government officials or regulators.	10
		Training Infrastructure	Availability of in-house training facilities, e-learning modules, or dedicated centres for legal-tech training.	5
2.	**Technical Institution's Profile**	**Technical Partner's Institutional Standing**	The Technical Partner Institution must demonstrate strong academic standing, evidenced through NIRF rankings or accreditation by equivalent national	10

			bodies for technical and engineering institutions.	
		Technical Partner's Capabilities	Demonstrated technical expertise, R&D infrastructure, and implementation capabilities.	10
		Collaboration Plan	Clarity and plausibility of the proposed collaboration structure, including roles of the technical partner, areas of technical support, and feasibility of delivering the policy–technical research mandate.	10
3.	**Presentation**	**Demonstrable execution capacity and Implementation roadmap**	Quality of presentation, clarity of vision, demonstrable capacity to execute the proposed CoE structure, implementation roadmap, and ability to respond to evaluation committee queries during the interview process.	20
TOTAL = 100				

Selection Process

- All applications shall be evaluated through a transparent, multi-stage process.
- Stage I shall comprise eligibility screening by an Eligibility Screening Committee to verify compliance with the minimum eligibility criteria specified in this Call for Proposals.
- Applications found eligible shall be considered for Stage II evaluation for shortlisting by an Evaluation Committee against the prescribed evaluation parameters as in Serial No. 1 and 2 of the above table (Evaluation Framework and Selection Process).
- Stage III shall consist of a presentation by shortlisted applicants before the Selection Committee on the proposed CoE structure, methodology, and implementation roadmap. ***The presentation shall assess demonstrable execution capacity and shall carry a weightage of 20% of the total evaluation score and the remaining 80% of the score shall be allocated to the other evaluation parameters as in the table for Evaluation Framework and Selection Process***.
- Applicants will be required to submit supporting documentation for verification during the evaluation process.
- Up to three (3) proposals may be selected. In case of more than one selection, consideration will be given to promote regional diversity in establishing the CoEs.

VII. Mode of Application

The Principal Investigator shall send application through email (*coe-cyberlaws@meity.gov.in*) in the prescribed format as in Annexure-I.

Annexure I - Proforma for Submission of Proposals

Sl. No.	Item	Details
1.	**CoE Title**	
2.	**Applicant Category**	● Central / State Government Law Universities ● Law Department within other Universities, accredited under the UGC framework.
3.	**Objectives of Proposed CoE**	
4.	**Summary of the Proposal**	
5.	**Principal Investigator**	● Name, address, and contact details ● Citizenship proof ● Employment letter from the institution
6.	**Co-Investigator(s)**	● Name, address, and contact details ● Citizenship proof ● Employment letter from the institution
7.	**Details of the Proposal**	● Aim and Scope of the Project ● Detailed description of the proposal ● Mission and Impact Alignment ● Overview of the institution's academic profile, research capabilities, infrastructure, relevant departments/centres, and prior experience in cyber law,

		technology policy, or related domains. ● Relevant accreditation certificates under the UGC framework. ● Detailed project plan, deliverables and timelines ● Bio-data of PI/Co-PI ● List of current or past projects of the PI/Co-PI/technical partner ● Documentation of previous collaborations, contribution to legislative drafting, capacity-building initiatives, or research engagement with central/state ministries, departments, or regulatory bodies. ● Certificate from the Principal Investigator (on the letter head of the Lead Institution) ● Endorsement by the Head of the Institution ● Letter of intent with the technical partner(s)
10.	**Break-up of sources of balance cost** (including share of partner institutions in the total cost, substantiated with letters/agreements)	

11.	**Other information**	• Infrastructural facilities available at the host institution (Annexure IV) • Infrastructural facilities available at the technical partner institution (Annexure V) • Availability of equipment which are relevant for the project (Annexure VI)
12.	**Details of functioning of CoE**	
13.	**Proposed costs and details**	• Proposed costs (Annexure II) • Detailed breakdown (Annexure III)

Annexure II - Proposed Costs

Sl. No.	**Item**	**Amount (₹)**	**1st Year**	**2nd Year**	**3rd Year**	**4th Year**	**5th Year**	**Total**
1.	Capital Expenditure							
2.	Manpower							
3.	Consumables							
4.	Programme Activities - Outreach, Training and Dissemination							
5.	Travel							
6.	Institutional Overhead Charges							
	Total							

Annexure III - Details of Costs of Various Components

a) Capital Expenditure

Sl. No.	Name of the Equipment	Number	Amount (₹) 1st Yr	2nd Yr	3rd Yr	4th Yr	5th Yr	Total
1.								
2.								

**Including transport, insurance and installation charges.*

b) Manpower Cost

Sl. No.	Designation / Numbers	Monthly Emoluments	Amount (₹) 1st Yr (m.m.*)	2nd Yr (m.m.)	3rd Yr (m.m.)	4th Yr (m.m.)	5th Yr (m.m.)	Total (m.m.)
1.								
2.								

**Man months to be given within brackets before the budget amount.*

c) Cost of Consumables

Sl. No.	Item	Quantity & Cost	Amount (₹) 1st year	2nd year	3rd year	4th year	5th year	Total
1.		Quantity						
2.		Total cost						

d) Programme Activities - Outreach, Training and Dissemination

Sl. No.	Item	Quantity & Cost	Amount (₹) 1st year	2nd year	3rd year	4th year	5th year	Total
1.								
2.								

d) Travel Cost

Sl. No.	Travel (Domestic / International)	Justification	Amount (₹) 1st year	2nd year	3rd year	4th year	5th year	Total
1.								
2.								

ANNEXURE IV - Infrastructural Facilities Available at the Host Institution

ITEM	YES	NO	Not Required
a) Workshop			
b) Water & Electricity			
c) Standby power supply			
d) Laboratory Space & furniture			

e) Air-Conditioned room for equipment			
f) Telecommunication			
g) Transportation			
h) Administrative & Secretarial support			
i) Library facilities			
j) Computational facilities			
k) Any other (Please mention)			

Annexure V - Infrastructural Facilities Available with the Technical Partner(s)

ITEM	**YES**	**NO**	**Not Required**
a) Workshop			
b) Water & Electricity			
c) Standby power supply			
d) Laboratory Space & furniture			
e) Air-Conditioned room for equipment			

f) Telecommunication			
g) Transportation			
h) Administrative & Secretarial support			
i) Library facilities			
j) Computational facilities			
k) Any other (Please mention)			

Annexure VI - Availability of equipment which are relevant for the project

Sl. No.	**Name of the Equipment and Accessories**	**Details**
1.		
2.		
3.		
4.		

*****