Response by the Centre for Information Policy Leadership to the Ministry of Electronics and Information Technology's Consultation on its AI Governance Guidelines Development Report

Submitted February 27, 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Ministry of Electronics and Information Technology (MeitY)'s Consultation on its AI Governance Guidelines Development Report. CIPL has closely followed India's efforts to guide the development of a trustworthy and accountable AI ecosystem in India and appreciates the work undertaken by the Subcommittee on AI Governance and Guidelines Development to publish the "Report on AI Governance Guidelines Development".[2]

For more than 20 years, CIPL has been a thought leader on organisational accountability and a risk-based approach as key building blocks of smart regulation, responsible governance, and use of data, as well as accountable development and deployment of AI. CIPL's "Ten Recommendations for Global AI Regulation" proposes a layered, three-tiered approach to AI regulation that would protect fundamental human rights and minimise the potential risks of harm to both individuals and society, while enabling the responsible development and deployment of AI.[3] Our benchmarking "report, "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework", outlines best practices and case studies on how 20 leading organisations are responsibly developing and deploying AI through the lens of CIPL's Accountability Framework.[4] CIPL's recent discussion paper, "Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators", considers key privacy and data protection concepts and explores how

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] Ministry of Electronics and IT (MeitY), "Report on AI Governance Guidelines Development", January 6, 2025, https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf

[3] CIPL, "Ten Recommendations for Global AI Regulation", October 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ten_recommendations_global_ai_regulation_oct2023.pdf.

[4] CIPL, "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework", February 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf

they can be effectively applied to the development and deployment of generative AI models and systems.[5]

CIPL commends the Subcommittee for proposing a whole-of-government approach to AI governance that fosters coordination among government agencies and invites collaboration with nongovernmental experts. CIPL also appreciates the Subcommittee's focus on clarifying how existing laws already apply to AI systems and identifying any gaps, and its recommendation for outcome-focused regulations oriented toward minimising risks while enabling the enjoyment of AI's benefits.

CIPL recommends that the Subcommittee and any work groups established pursuant to its recommendations adopt a flexible, risk-based approach that assesses the potential benefits and harms of AI technologies in the context of specific use cases. Overly broad and rigid categories of high-risk AI systems risk capturing potentially low-risk uses of AI and creating undue burden for both developers and deployers. Furthermore, CIPL supports the adoption of risk management practices for uses of AI that impact the rights and safety of the public. As noted in our white paper "Ten Recommendations for Global AI Regulation", any regulatory approach to AI should seek to protect fundamental human rights and minimize risks to individuals and society, while enabling the development and use of AI for the benefit of both. Such an approach, grounded in principles of organisational accountability, would facilitate practical protective measures that are proportional to the risks and benefits of AI systems. For example, the Subcommittee should consider the importance of enabling use cases that benefit individuals and society, such as fraud prevention, cybersecurity, and anti-money laundering.

CIPL also recommends that the Subcommittee define key concepts addressed in the report—most importantly, "artificial intelligence." To foster clarity and interoperability with rules and guidance from other jurisdictions, the Subcommittee may want to consider aligning to the definition of "AI system" published by the Organisation for Economic Co-operation and Development (OECD) in 2023. [6]

Please find CIPL's feedback to the specific recommendations of the Subcommittee:

1. **Recommendation 1: To implement a whole-of-government approach to AI Governance, MeitY and the Principal Scientific Adviser should establish an empowered mechanism to coordinate AI Governance.**
    - CIPL welcomes this recommendation. The Subcommittee suggests that the body "may be headed by the Principal Scientific Adviser." While it is sensible for one individual to chair the new body, CIPL encourages the government to also specify an agency to serve as the lead for coordinating the body's activities. At the same time, this agency should not act as a "super agency" for AI, but rather a coordinator to help reduce the potential for confusion within organisations and help streamline interactions and communications with the

[5] CIPL, "Applying Data Protection Principles to Generative AI: Practical Approaches for Organisations and Regulators", December 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf

[6] The updated 2024 OECD "Recommendation of the Council on Artificial Intelligence" defines "AI systems" as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

government. With respect to matters regarding the processing of personal data, data protection authorities should be the lead and chief point of contact for organisations, collaborating with other regulators where appropriate.

- CIPL supports the Committee being comprised of both official members (i.e., from government agencies and departments) and non-official members (i.e., from industry, academia, and civil society). CIPL's research for our benchmarking report has demonstrated the importance of representation from a diverse range of perspectives and expertise.[7]

2. **Recommendation 2: To develop a systems-level understanding of India's AI ecosystem, MeitY should establish, and administratively house, a Technical Secretariat to serve as a technical advisory body and coordination focal point for the Committee/ Group.**
    - CIPL commends this recommendation and supports establishing a Technical Secretariat to serve as a technical advisory body and coordination focal point for the Committee. We have long seen the added value and benefit of ensuring sufficient technical expertise and understanding, particularly among regulators, and have advocated for greater engagement of subject matter experts who have practical experience. Given the outlined duties of the Secretariat in the report, CIPL believes that this role would be critical to continuously educate the Committee on AI-related matters and keep abreast of a rapidly changing landscape. Once the Technical Secretariat is established, CIPL would be pleased to contribute our expertise to its work.

3. **Recommendation 3: To build evidence on actual risks and to inform harm mitigation, the Technical Secretariat should establish, house, and operate an AI incident database as a repository of problems experienced in the real world that should guide responses to mitigate or avoid repeated bad outcomes.**
    - CIPL commends MeitY's efforts to establish an AI incident database that will act as a repository of problems and help guide mitigation efforts for future incidents. CIPL's report on accountable AI programs outlines a number of similar best practices that leading organisations have implemented. For example, several organisations have already created centralized inventories that not only include records of an organisation's existing AI projects, products, and services but also log and track all risk assessments. Another has created an internal database as its "mitigation library" to store documentation on previously employed mitigation measures for various AI-related risks. Please see CIPL's response to Recommendation 4 for additional perspectives on AI risk categorisation.
    - CIPL appreciates the distinction that the Subcommittee has drawn between cybersecurity incidents and the broader concept of AI incidents, and the suggestion that the database be used chiefly as a tool to foster learning and more effective mitigation.
    - CIPL suggests the Subcommittee establish a clear, concise, and focused definition of AI incidents that balances comprehensiveness with simplicity.

---

[7] CIPL, "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework", February 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf

- The Subcommittee may want to consider providing a materiality threshold or criteria to help organisations prioritize the incidents most relevant for voluntarily sharing, which in turn helps focus attention on the highest risk problems and most effective mitigations. CIPL suggests that the Subcommittee carefully consider if CERT-IN is the appropriate entity to manage the AI incident database, given that CERT-IN specializes in required cybersecurity incidents, which differs from what is proposed in the report.

4. **Recommendation 4: To enhance transparency and governance across the AI ecosystem, the Technical Secretariat should engage the industry to drive voluntary commitments on transparency across the overall AI ecosystem and on baseline commitments for high capability/widely deployed systems.**
   - Transparency is an essential aspect of building trust and garnering credibility in developing and deploying AI technologies, particularly with the widespread availability and use of generative AI. Transparency is also a key feature of emerging regulatory guidance and requirements. CIPL agrees that truly accountable organisations should strive to be transparent about their AI practices with both internal and external stakeholders, and our research demonstrates that leading organisations are already trying to implement this in practice. Many of these organisations are tailoring the level and type of information provided based on the target audience (e.g., within the organisation, business partners or third parties, regulators, end users, etc.). Transparency should not come at the expense of other important factors, such as usability, functionality, and data security, or create additional burdens for users. The level of transparency should be balanced not only with the need to protect IP rights, copyright, and confidential information, but also with the vulnerabilities of systems and the potential net societal benefits from AI. Risk assessments can help organisations properly weigh these considerations and determine a sufficient level of transparency. Please refer to our report on accountable AI governance and its section on transparency for more best practices on transparency.[8]
   - While the AI ecosystem involves several entities as described in the report, it is still unclear how AI and AI systems will be defined by the Subcommittee. Thus, as mentioned previously, CIPL believes it will be helpful for the Subcommittee to define key terms and clarify the criteria for risk classifications in alignment with existing frameworks and definitions. As noted above, CIPL recommends that the definition for "AI systems" be more closely aligned with the most frequently used international standards, such as the OECD definition.[9] Ensuring alignment of key terms will ensure consistency and interoperability between regulatory approaches while enhancing consumer protections and supporting companies operating globally.

---

[8] CIPL, "Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework", February 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf

[9] The updated 2024 OECD "Recommendation of the Council on Artificial Intelligence" defines "AI systems" as "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

- The list of proposed voluntary commitments specifies "peer review by third-party qualified experts". CIPL suggests that the Subcommittee exercise caution regarding third-party review, testing, or auditing requirements, particularly as there are currently no standards for this emerging industry. The Subcommittee should consider how internal self-assessments may also play an important role in effective transparency and AI governance.
- **Establishment of a potential baseline framework for medium-to-high risk systems (sub-point under Recommendation 4).** The report suggests that there may be a need for a baseline framework that applies to the development and deployment of AI systems that are considered "medium-to-high risk" yet does not specify the criteria for such risk classification. CIPL encourages the Subcommittee to define the criteria for further clarity and consider aligning to existing frameworks to encourage interoperability and convergence. At the same time, any such classification should be tied to use cases rather than specific technologies, and the presumption of classification as medium or high risk should be rebuttable based on contextual risk assessments.

5. **Recommendation 5: The Technical Secretariat should examine the suitability of technological measures to address AI-related risks.**
   - As a forthcoming CIPL white paper documents, technical solutions, such as privacy-enhancing technologies (PETs) and privacy-preserving technologies (PPTs), can play an important role in maximizing the benefits of AI while preserving privacy and security by integrating them into the design and architecture of AI systems. These technologies – including homomorphic encryption, federated learning, trusted execution environments, secure multi-party computation, differential privacy, and synthetic data – are gaining increased attention and investment from both industry and regulators as options for addressing privacy concerns in AI models. Regulators and data-using organisations across many jurisdictions are exploring the extent to which PETs can mitigate risk. CIPL encourages the Subcommittee to consider and provide guidance regarding the suitability of technical measures, such as PETs/PPTs, to address AI-related risks.

6. **Recommendation 6: Form a sub-group to work with MEITY to suggest specific measures that may be considered under the proposed legislation like Digital India Act (DIA) to strengthen and harmonise the legal framework, regulatory and technical capacity and the adjudicatory set-up for the digital industries to ensure effective grievance redressal and ease of doing business.**
   - CIPL agrees with the Subcommittee that existing laws can and should be applied and enforced to cover various areas of AI-related risks, and we commend the Subcommittee for performing an extensive gap analysis to see where existing laws already deal with the risks and harms of AI systems. As outlined in the report, many existing Indian laws provide a robust foundation for AI, and they must continue to be adapted to remain fit for purpose alongside developments in technology. CIPL encourages MeitY to consider releasing guidance on relevant legislation to provide clarity on how key requirements may be enforced for AI. We have seen numerous regulators do so, particularly with the rapid advancement of generative and general-purpose AI (e.g., CNIL, ICO, EDPB, ANPD, etc.). It

will also be important to consider global convergence and harmonisation to reduce the potential for contradictory or divergent legal frameworks.

- As noted earlier, should the need for AI-specific regulation arise, it is crucial that MeitY creates a flexible, adaptable framework that adopts a risk-based approach and includes relevant descriptions for AI applications that benefit individuals and society (e.g., fraud prevention, cybersecurity, anti-money laundering, etc.). In CIPL's "Ten Recommendations for Global AI Regulation", we propose that any AI regulation should be technology-neutral, as well as principle- and outcome-based. This would prevent the framework from becoming outdated due to technological changes, overly prescriptive or specific to individuals or business models, and ensure the required outcomes (e.g., fairness, non-bias, transparency, accuracy, security, human oversight, etc.) through risk-based, verifiable internal policies, procedures, and controls that are appropriate in their specific contexts. Again, any regulatory approach to AI should take a holistic, risk-based approach that provides non-exhaustive criteria to assist organisations in determining the likelihood and severity of any harm resulting and the measures required to mitigate it. Assessing and understanding the potential impact of their AI applications allows organisations to tailor their mitigations to the actual risks and avoid the implementation of unnecessary measures.