Summary: Submissions on the AI Governance Guidelines Development Report

Introduction

The Data Security Council of India (DSCI) welcomes the efforts of the Office of the Principal Scientific Adviser (PSA) and the Subcommittee on AI Governance and Guidelines Development in formulating AI governance principles for India. As a leading think tank and industry association focused on data protection, cybersecurity, and privacy, DSCI broadly supports the principles-based approach proposed in the Report while offering specific observations to enhance its effectiveness.

Dynamic and Contextual AI Governance

DSCI commends the inclusion of globally recognized AI governance principles in the Report. However, considering AI's diverse applications and rapidly evolving nature, DSCI recommends:

- The governance structure may remain dynamic, allowing for gradual refinements as AI technologies evolve.
- Different types of AI (Generative AI, Narrow AI, Agentic AI) may require varying levels of governance based on their capabilities and risk profiles, hence allow for an adaptive framework for AI governance.
- Following global examples like the EU AI Act and OECD AI Principles, India's governance framework may adopt a risk-based approach that imposes stricter oversight on high-risk AI applications while enabling innovation for lower-risk systems.

Key Recommendations on AI Governance Principles

1. Transparency

While endorsing transparency as a core principle, DSCI suggests:

- Transparency requirements may be balanced with intellectual property protection to encourage innovation.
- Different levels of information may be provided to end-users (e.g., AI-generated content labeling) versus regulators (e.g., structured documentation).
- Emphasize AI safety benchmarking and testing models to ensure transparency without compromising commercial confidentiality.

2. Accountability

DSCI recommends:

- Accountability frameworks may consider the deployment environment, technological advancement, and stakeholder roles.
- Similar to Data Principals under the DPDP Act, end-users may exercise due diligence when using AI tools, particularly regarding misinformation and copyright concerns.

3. Safety, Reliability, and Robustness

To operationalize these principles effectively, DSCI suggests:

- Establishing structured evaluation frameworks tailored to India's unique context, this would help assess AI models against predefined performance, security, and ethical criteria.
- Promoting standardized testing protocols and sector-specific guidelines, especially for high-risk AI applications.
- Incentivizing AI developers to conduct comprehensive safety evaluations before deployment.

4. Privacy and Security

Acknowledging the unique privacy challenges posed by AI systems, DSCI recommends:

- Traditional data protection concepts (data deletion, consent withdrawal) may not be technically feasible for advanced AI models that process patterns rather than storing discrete personal data.
- Explore AI-specific privacy solutions such as differential privacy, federated learning, and privacy-enhancing computation.

Specific Recommendations on Implementation

1. Governance Structure

DSCI supports the establishment of an Inter-Ministerial Committee and Technical Secretariat at MeitY, with additional suggestions:

- **India-Centric Safety Metrics**: Develop localized AI safety benchmarks that address India's unique challenges, including linguistic diversity and sector-specific applications.
- **Collaborative Development**: MeitY's Technical Secretariat may coordinate with industry, academia, and global AI governance bodies to develop these safety benchmarks.

2. AI Incident Reporting and Database

While supporting the creation of an AI Incident Database, DSCI recommends:

- **Clear Scope Definition**: Distinguish AI incidents from cybersecurity incidents, recognizing their unique characteristics involving bias, discrimination, misinformation, and ethical concerns.
- **Appropriate Institutional Oversight**: Consider whether a dedicated AI-focused body (such as the proposed AI Safety Institute) might be better positioned to manage AI-specific risks.
- **Voluntary, Trust-Based Approach**: Encourage voluntary reporting without fear of punitive consequences to foster collaborative learning.
- **Responsible Disclosure**: Ensure that publicly accessible information protects the identity of reporting organizations to prevent reputational risks.

Conclusion

DSCI believes that by anchoring AI governance in foundational principles while allowing for contextual implementation, India can develop a framework that ensures safety and ethical integrity while remaining adaptive to technological advancements. This balanced approach would encourage responsible AI innovation through a governance model that is risk-sensitive, scalable, and aligned with global best practices while addressing India's unique requirements.

The Council remains committed to supporting the government's efforts in developing a robust AI governance framework that fosters innovation while ensuring responsible AI deployment across India's digital ecosystem.