INDIALAW

REGULATORY

# Fortifying the Digital Frontier: SEBI’s Cybersecurity Advisory and NCCL’s Response to AI-Driven Threats

Introduction The rapid proliferation of advanced artificial intelligence tools capable of autonomously identifying and potentially exploiting cybersecurity vulnerabilities has compelled India’s financial regulators and market infrastructure institutions to respond with urgency and precision. Two recent circulars — one from NCCL and one from SEBI — address the cybersecurity risks posed by emerging AI-driven vulnerability detection […]

AUTHOR Aditi Rana, Tanvi Dalvi

PUBLISHED 12 May 2026

## Introduction

The rapid proliferation of advanced artificial intelligence tools capable of autonomously identifying and potentially exploiting cybersecurity vulnerabilities has compelled India's financial regulators and market infrastructure institutions to respond with urgency and precision. Two recent circulars — one from NCCL and one from SEBI — address the cybersecurity risks posed by emerging **AI-driven vulnerability detection tools**.

On 7th May 2026, the National Commodity Clearing Limited ("NCCL") issued Circular No. NCCL/TECHNOLOGY-012/2026. On 5th May 2026, the Securities and Exchange Board of India ("SEBI") issued Circular No. HO/13/19/12(1)2026-ITD-1_CIMGI/10873/2026. Both circulars address the cybersecurity risks arising from AI-driven vulnerability detection tools, with particular reference to tools such as Claude Mythos.

These circulars represent a significant development in India's evolving cybersecurity governance framework and impose substantive compliance obligations upon all **Regulated Entities ("REs")** and relevant market participants operating within the securities market ecosystem.

Table of contents



## Background and Regulatory Context

The securities market ecosystem in India encompasses a broad and interconnected network of **market infrastructure institutions ("MIIs")**, qualified registrar and transfer agents ("QRTAs"), stock exchanges, depositories, clearing corporations, mutual funds, portfolio managers, and other intermediaries.

The inherent interdependency among these participants creates a systemic vulnerability: a cyber breach at any one node may propagate cascading consequences across the entire market infrastructure. It is against this backdrop that NCCL and SEBI have issued their respective communications.

The SEBI circular expressly invokes SEBI's statutory authority under **Section 11(1) of the Securities and Exchange Board of India Act, 1992**, to protect investor interests and regulate the orderly functioning of securities markets.

The NCCL circular separately requests its clearing members to take note of the advisory and read it with applicable SEBI circulars, including the Cybersecurity and Cyber Resilience Framework and subsequent SEBI updates.

## Nature of the Threat: AI-Driven Vulnerability Detection

The circulars expressly identify AI-driven vulnerability detection tools, exemplified by **Claude Mythos**, as instruments capable of introducing heightened risk exposure to Regulated Entities.

Unlike conventional penetration testing mechanisms, such tools operate with considerable speed and at scale, thereby enabling the identification and potential exploitation of systemic vulnerabilities in a *compressed timeframe*.

The regulators further note that the deployment of such tools raises serious concerns regarding data confidentiality, the integrity of critical applications, and the reliability of outputs generated thereby. The gravity of this assessment is underscored by the establishment of a dedicated inter-institutional task force, named **"cyber-suraksha.ai,"** to coordinate a uniform regulatory and technical response.

## The Cyber-Suraksha.ai Task Force: Mandate and Governance

Constituted by SEBI with representation from MIIs, QRTAs, all Qualified Regulated Entities ("QREs"), and other relevant stakeholders, the **cyber-suraksha.ai task force** has been entrusted with a four-pronged mandate:

1. Examining cybersecurity risks arising from AI-based models and formulating uniform mitigation strategies.
2. Facilitating the exchange of threat intelligence and best practices in vulnerability management.
3. Reporting cyber incidents and significant attack vectors on a priority basis.
4. Reviewing the cybersecurity posture of third-party application service providers, including empaneled vendors.

The task force has already convened a meeting with MIIs and QRTAs and, on the basis of the deliberations therein, issued a detailed advisory set forth in **Annexure-A** to the circulars.

## Key Compliance Obligations Under Annexure-A

The advisory contained in Annexure-A is comprehensive in scope and prescribes a series of **immediate and ongoing compliance measures**.

### Patching and Vulnerability Assessments

All Regulated Entities are directed to apply the **latest security patches** to operating systems and applications on an immediate basis, with virtual patching serving as an interim safeguard where conventional patches remain unavailable.

Entities are further required to conduct regular vulnerability assessments using conventional and suitable AI-based vulnerability assessment tools wherever possible, and security audits in accordance with SEBI's **Cyber Security and Cyber Resilience Framework ("CSCRF")**.

### Third-Party Vendor Risk Assessments

Third-party vendors, particularly those providing commercial off-the-shelf solutions to market members, are required to undertake **comprehensive risk assessments** specific to the deployment of AI-led vulnerability detection models and implement appropriate technical safeguards, including:

- Updated patches
- Vulnerability and penetration testing ("VAPT")
- Continuous monitoring
- System hardening measures

### Change Management and API Security

The advisory prescribes rigorous **change management protocols**, under which even minor system changes should be supported by full documentation, impact analysis, structured review, rigorous testing, and secure deployment.

It also requires **API security controls**, including:

- Regularly updated API and application inventories
- Strong authentication and authorization
- Least-privilege access
- Rate limiting and throttling
- A strict whitelist-based approach

### System Hardening

REs are also expected to implement **system hardening** through the following measures:

- Secure configurations
- Disabling unnecessary services and default accounts

- Enforcing least-privilege and Zero Trust Network Architecture ("ZTNA") controls to reduce the attack surface

### SOC Monitoring and M-SOC Integration

With respect to Security Operations Centre ("SOC") monitoring, all eligible Regulated Entities not yet onboarded to the **Market SOC ("M-SOC")**, established jointly by NSE and BSE, are directed to expedite their integration with that centralized security platform.

Additional SOC-related obligations include:

- SOC alerts, including low-priority alerts, are required to be adequately examined.
- REs are encouraged to implement tested **SOAR playbooks** integrated with SIEM solutions wherever feasible.
- MIIs are required to conduct awareness and handholding programmes, including periodic workshops, to facilitate smooth onboarding and integration with M-SOC.
- Entities must periodically update asset inventories and Software Bills of Materials for all critical applications, including open-source stacks.

### Risk Assessments and Long-Term AI Planning

The advisory requires periodic and **scenario-based risk assessments** under the CSCRF framework, including assessment of internal and external cybersecurity risks in the RE's IT environment and consideration of AI-based model capabilities as a risk scenario.

MIIs and other REs are also required to:

- Seek guidance from their respective IT committees
- Prepare a long-term plan for AI usage in detection and autonomous/agentic mitigation
- Recalibrate risks for AI-accelerated threats
- Pursue AI-augmented SOC transformation
- Adopt continuous vulnerability management using AI tools

## Legal Implications and Enforcement Dimension

The circulars are *not* merely advisory in character. Having been issued in exercise of SEBI's powers under **Section 11(1) of the SEBI Act, 1992**, the obligations prescribed therein carry statutory authority.

Non-compliance may expose Regulated Entities to regulatory scrutiny, enforcement proceedings, and reputational consequences.

Entities are accordingly advised to treat the Annexure-A directives as **enforceable compliance obligations**, to document their implementation measures meticulously, and to align their long-term technology governance strategies with the broader mandate for AI-augmented SOC transformation and autonomous threat mitigation.

## Conclusion

The NCCL and SEBI circulars of May 2026 represent a **material regulatory development** in India's regulatory approach to artificial intelligence and cybersecurity within the financial markets sector.

By explicitly recognizing AI-driven vulnerability detection as a material systemic risk, and by prescribing a structured, cross-institutional compliance architecture in response, SEBI and market infrastructure institutions have signalled that AI-related cyber risk must now be embedded into vulnerability management, vendor oversight, SOC monitoring, API governance, risk assessment, and long-term cyber-resilience planning.

For more details, write to us at: contact@indialaw.in

**Reference:**

Circular No. [NCCL/TECHNOLOGY-012/2026] [May 07, 2026] Advisory on Emerging Advanced Artificial Intelligence (AI) Tools for Vulnerability Detection (like Mythos)

## Related Practice Areas