BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR I FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2026-034

To : **ALL BANGKO SENTRAL-SUPERVISED INSTITUTIONS (BSIs)**

Subject : **Recommendations for Managing Emerging Risks Arising from Frontier Artificial Intelligence Systems**

The rapid advancement of frontier artificial intelligence (AI) systems introduces significant cybersecurity risks that demand immediate attention. Such systems are described as having the ability to identify software vulnerabilities, generate exploit pathways, and execute multi-stage cyberattacks with minimal human intervention. While access to these systems remains restricted and controlled, their emergence signals a shift toward increasingly adaptive and scalable cyber threats. Accordingly, BSIs are reminded that similar AI-enabled capabilities may eventually be leveraged by malicious actors to target financial systems, third-party service providers, and critical infrastructure.

BSIs must ensure that their cybersecurity and technology risk management frameworks, as well as cyber hygiene practices, remain robust and resilient against the increasing speed, scale, and sophistication of AI-enabled threats. Sound practices for asset management, identity and access management, vulnerability management, security monitoring, incident response, and third-party risk management, among others, must be consistently implemented and maintained. In line with this, specific recommendations on frontier AI systems include the following:

1. ***Enhance attack surface visibility.*** Strengthen visibility across the BSI's attack surface by maintaining accurate and up-to-date inventories of externally reachable assets, cloud services, identities, critical applications, and software dependencies, including third-party and open-source systems/components.
2. ***Strengthen foundational security controls***. Fortify foundational controls across all environments through strong credential hygiene, Multi-Factor Authentication (MFA) for critical systems and assets, and strict least-privilege access with device hardening baselines, among others.
3. ***Reduce exposure through proactive attack surface controls.*** Implement proactive attack surface reduction measures, including adopting micro-segmentation and zero trust security controls, compressing patch timeliness, replacing or upgrading end-of-life systems/platforms and limiting unnecessary internet exposure of systems.
4. ***Reinforce authentication measures.*** Adopt Multi-Factor Authentication (MFA) using hardware security keys (e.g., FIDO2/WebAuthn keys), Smart Cards, or hardware-backed Certificate-Based Authentication. In line with this, discontinue the use of knowledge based (passwords) or communication-based (SMS/Push) authentication for all administrative and privileged access to mitigate AI-driven social engineering.
5. ***Leverage AI-enabled defensive capabilities.*** Adopt AI-enabled cybersecurity controls and capabilities for patch management, continuous threat hunting, exposure management, and security orchestration. Deploy virtual patching controls to block exploit paths, particularly for critical systems, before updating the underlying software.
6. ***Enhance readiness and response capabilities.*** Review and enhance the Business Continuity Management framework and Business Continuity Plans to ensure preparedness for AI-enabled threats.

The foregoing recommendations are consistent with the risk-based framework for information technology and cybersecurity risk management prescribed under Section 148 of the Manual of Regulations for Banks (MORB) and Sections 147-Q/145-S/142-P/126-N of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI). They are intended to complement and strengthen existing risk management and control measures, thereby ensuring that emerging risks are effectively identified, assessed, and mitigated.

Finally, BSIs are recommended to formally develop their own AI Governance Framework, proportionate to the nature, extent, scale, complexity, and materiality of their AI systems, as well as the institution's overall operational complexity and risk profile, following the principles set forth under BSP Memorandum No. M-2026-031 dated 24 June 2026.

For information and guidance.

LYN I. JAVIER
Deputy Governor

Digitally signed by Lyn I. Javier
Date: 2026.07.06 10:53:25 +08'00'

06 July 2026