● Month ●, 2026

To: ●●

●● Bank

Request for the Review and Enhancement of Cybersecurity Management Frameworks in Light of the Evolving Threat Landscape Posed by Frontier AI

In recent years, advances in so-called Frontier AI have significantly accelerated the pace at which vulnerabilities can be discovered and attack code can be generated. As a consequence, vulnerabilities that were previously difficult to identify may now be discovered in substantial numbers within a short timeframe, and the time lag between the identification of a vulnerability and its exploitation in actual attacks may be significantly shortened.

Against this backdrop, ensuring the effectiveness of cybersecurity measures at financial institutions requires not only financial institutions themselves to take appropriate action, but also service providers supporting financial institutions to implement appropriate measures.

Accordingly, we respectfully request that such service providers promptly review and, where necessary, enhance their IT and cybersecurity management frameworks in light of the evolving threat landscape posed by Frontier AI.

1. Illustrative Short-Term Measures for Service Providers Supporting Financial Institutions

For reference, examples of short-term measures are set out below. Taking into account your organization's risk profile and IT/cybersecurity management framework, you are requested to proactively assess and implement any measures deemed necessary.

(Addressing a Large Volume of Vulnerabilities)

i. Treat vulnerability management and the sustainable provision of critical services as management priorities in light of the evolving threat landscape posed by Frontier AI.

ii. Identify the services and/or IT systems that should be accorded priority in implementing measures.

iii. With respect to the identified assets, assess and remediate any technical debt, including unapplied patches, unsupported products, unnecessary externally exposed services, and unnecessary accounts or privileges.

iv. Confirm the availability of the human resources necessary for patch deployment and impact assessments, the support arrangements of outsourced service providers, and personnel capable of responding to emergencies.

v. Review maintenance and support agreements, allocation of responsibilities, and emergency communication and response arrangements with vendors, maintenance providers, contractors, subcontractors, and any other relevant third parties engaged by your organization.

vi. Determine the order of priority for patch deployment based on such factors as the degree of impact on critical services, the severity of the vulnerability, and the likelihood of exploitation.

vii. Where prompt patch deployment is not feasible, consider alternative risk-mitigation measures, including access controls, enhanced monitoring, protective measures using web application firewall (WAF) functionality, suspension of relevant functions, and network segmentation.

viii. In preparation for possible suspension of prioritized services or IT systems, functional restrictions, or disconnection from external networks, review the business continuity plan (BCP), emergency response framework, service suspension decision-making process, and recovery procedures.

ix. Review communication and information-sharing arrangements with financial institutions, maintenance vendors, contractors, subcontractors, industry associations, security-related bodies, and other relevant organizations.

2. Notification to Financial Institutions

Where any material vulnerability, cyberattack-related damage, indicators of compromise, risk of service suspension, or any other matter that may affect services provided to financial institutions is identified, and there are reasonable grounds to believe that such services may be impacted, the relevant financial institution(s) should be notified promptly, even if the precise scope or extent of the impact has not yet been fully determined.

3. For Reference

Financial Services Agency: “Regarding the Request Concerning Short-Term Responses by Financial Institutions, etc. in Light of the Evolving Threat Landscape Posed by Frontier AI” (Japanese Only)

URL: https://www.fsa.go.jp/news/r7/sonota/20260522-5/20260522.html

Bank of Japan: “Regarding the Request Concerning Short-Term Responses by Financial Institutions, etc. in Light of the Evolving Threat Landscape Posed by Frontier AI” (Japanese Only)

URL: https://www.boj.or.jp/finsys/release/frel260522a.htm

Yours faithfully,

End