22nd May 2026

To the Representatives of the Relevant Businesses Operators

Request Regarding “Short-Term Measures for Financial Institutions in Response to Changes in Threat Posed by Frontier AI”

As AI technologies continue to advance rapidly, their use in cyberattacks is accelerating both the speed and scale of such attacks, thereby heightening cybersecurity risks. In particular, the so-called “frontier AI” is expected to significantly enhance capabilities for identifying and remediating vulnerabilities, making it essential to take appropriate measures.

Against this backdrop, the Financial Services Agency (FSA) convened a Public-Private Coordination Meeting on Strengthening Cybersecurity Measures in the Financial Sector Against AI-Related Threats on April 24. Based on the discussions at the meeting, a working group meeting involving financial institutions, IT service providers, relevant government bodies, the Bank of Japan, and other stakeholders was held on May 14 to develop a shared understanding of AI-related threats and to examine appropriate measures.

In anticipation of a potential surge in vulnerability identification and patch releases, the working group has compiled the attached document titled “Short-Term Measures for Financial Institutions in Response to Changes in Threat Posed by Frontier AI.”

Financial institutions should implement the measures set out in the attachment with the direct involvement of senior management, particularly top executives. This request is based on the current circumstances, and it is important to continuously review and update the necessary measures in a timely and flexible manner considering developments in AI.

The FSA will also take forward its initiatives in line with the government-wide measure, “Strengthening Cybersecurity Measures in Light of Advances in AI

Capabilities (Project YATA-Shield)"[1] announced on May 18 by National Cybersecurity Office, while considering the characteristics of the financial sector.

[1] https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf

Short-Term Measures for Financial Institutions in Response to Changes in Threat Posed by Frontier AI

1. Background

In recent years, the advancement of so-called “frontier AI” has heightened concerns over the increasing sophisticated cyberattacks. Frontier AI is highly capable of identifying vulnerabilities and generating sophisticated exploit code. And it has been pointed out that frontier AI enables the rapid identification of vulnerabilities that were previously difficult to detect and significantly shortening the time between their discovery and exploitation. Furthermore, there is a growing concern that even inexperienced attackers may leverage frontier AI to carry out more sophisticated cyberattacks.

Given the possibility that many vulnerabilities may be identified and corresponding security patches released within a short period of time, financial institutions should urgently review and strengthen their capabilities across asset management, vulnerability management, patching, monitoring, and resilience, in order to ensure prompt and appropriate measures. Senior management should demonstrate leadership in driving these efforts, and make timely decisions, including those on the necessary resource allocation. Senior Management, including CIOs and CISOs, should be directly involved in the implementation of relevant measures.

It should also be recognized that these risks are not confined to internally developed systems, but may also extend to third-party software and services, including open-source components.

At the same time, according to a report by the UK AI Security Institute (AISI)[2], it has not yet been established whether frontier AI systems are capable of successfully attacking well-defended IT systems. In light of this, it remains essential to steadily implement fundamental cybersecurity measures in accordance with the FSA’s Guidelines on Cybersecurity for the Financial Sector.

[2] AI Security Institute (AISI), Our evaluation of Claude Mythos Preview’s cyber capabilities, https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

2. Short-Term Measures to be Taken by Financial Institutions

(Measures to a Large Volume of Vulnerabilities)

Financial institutions should promptly implement the following short-term measures[3]. These are intended as immediate measures; over the medium to long term, financial institutions should work toward more advanced approaches, such as the automation of vulnerability management. Responses to a large volume of vulnerabilities should not be limited to the measures outlined below. Each financial institution should proactively identify and implement additional necessary actions based on its own risk profile and cybersecurity management framework.

Furthermore, these measures cannot be completed within IT or cybersecurity functions alone; it is essential that top executives have an accurate understanding of frontier AI and an appropriate sense of urgency, and secures the necessary resources, including budget and personnel.

(1) Positioning the Measure to Frontier AI as a Management Priority

The evolving threats posed by frontier AI should not be regarded as issues limited to IT or cybersecurity functions. Top executives should recognize this as a company-wide priority and demonstrate commitment to ensuring close coordination across business units, risk management, IT and cybersecurity, finance and other relevant functions.

Under the leadership of top executives, it is essential that senior management, including CIOs and CISOs, be directly involved in formulating measure strategies, monitoring implementation status, and addressing related challenges on an ongoing basis.

[3] Financial institutions and related entities are expected to proceed with their responses, taking into account developments in the activities of AI model developers, with a timeframe of approximately one month as a general guideline.

(2) Identification of Priority Services and IT Systems

The large-scale identification of vulnerabilities is expected to significantly increase the workload associated with patching. However, it is not realistic to significantly expand existing IT resources in the short term. Accordingly, financial institutions should adopt a risk-based approach by identifying priority services and IT systems and allocating resources in a focused manner.

In particular, externally accessible IT systems supporting critical services, such as internet banking, should be prioritized. Where such systems are operated under shared or joint arrangements, it is essential to ensure a common understanding between users and service providers and to clearly define roles and responsibilities in advance.

(3) Resolution of Technical Debt in Identified Assets

For the priority services and IT systems identified in (2), financial institutions should review software and network configurations to ensure that patching targets can be promptly identified when vulnerabilities are identified. At the same time, technical debt should be reduced to the greatest extent possible, for example, by closing unnecessary network ports, removing redundant privileged accounts, and applying outstanding patches. These actions will both strengthen security and enable more efficient patching. Systems running on products that have reached end-of-support should be upgraded to supported versions, as patches will no longer be provided by vendors.

(4) Securing Personnel for Patching

To cope with the expected increase in vulnerabilities, financial institutions should review project plans related to priority services and IT systems and consider allocating additional personnel, including leveraging resources from other IT teams. In parallel, financial institutions should confirm that vendors responsible for patching have secured sufficient capacity to handle an increasing volume of vulnerabilities.

In addition, adequate resources should also be allocated for vulnerability triage. Where triage is conducted jointly with vendors, financial institutions should verify that sufficient vendor resources are in place.

(5) Verification of Vendor Maintenance Contracts

Many financial institutions outsource the maintenance and operation of the IT systems under their responsibility to vendors. Given that, it is important to ensure that patching activities are covered under existing maintenance contracts, and that roles and responsibilities are clearly defined. Financial institutions should also confirm that contracts allow for timely patching, including during nights and holidays. Furthermore, even where patching for many vulnerabilities arises simultaneously across multiple financial institutions, it is necessary to ensure that vendors have secured sufficient resources to perform patching in compliance with the service level agreements (SLAs) and service level objectives (SLOs[4]) defined in their contracts. At the same time, financial institutions should prepare scenarios in which vendor resources become constrained by establishing processes for prioritization and, where necessary, risk acceptance in the event of delays.

For IT systems provided under joint operating arrangements or by cloud service providers, it is necessary to ensure that contractual arrangements provide appropriate reporting to financial institutions on patching-related SLAs and SLOs, including their scope of application and implementation status.

(6) Adopting a Risk-Based Approach to Patching

Where many vulnerabilities are identified in the priority services and IT systems identified in (2), it may be difficult to address all of them. While prioritization has traditionally been based on CVSS[5] scores and the availability of exploit code, it should be noted that even low-scoring vulnerabilities are increasingly being exploited, and this trend is likely to accelerate with the advancement of frontier

---

[4] A Service Level Agreement (SLA) is a contract between financial institutions and vendors that defines service quality commitments, while a Service Level Objective (SLO) refers to internal targets established within an organization to achieve those commitments.

[5] CVSS (Common Vulnerability Scoring System) is a vulnerability assessment framework published by FIRST (Forum of Incident Response and Security Teams). In addition to Base Metrics that evaluate the intrinsic technical severity of a vulnerability, CVSS provides a score ranging from 0.0 to 10.0 based on factors such as the availability of exploit code and the potential threats within the target system environment. Guidelines for the Introduction of Vulnerability Assessment in Government Information Systems: Digital Society Promotion Practical Guidebook (DS-221)

AI. Moreover, exploit code may emerge immediately after vulnerabilities or patches are identified. Accordingly, financial institutions should assess the potential impact of vulnerabilities on their own services and IT systems—including the likelihood of exploitation—and prioritize measures on a risk basis, ensuring that higher-risk vulnerabilities are addressed promptly and thoroughly.

With regard to testing prior to patching, financial institutions should consider measures such as reasonably narrowing the scope of testing, after carefully balancing the risk of IT system failures due to insufficient testing against the risk of cyberattacks arising from unpatched systems.

(7) Strengthening Measures Beyond Patching

Where patching itself is difficult, or where it is not feasible to shorten the time required for patching in the priority services and IT systems identified in (2), it is necessary to strengthen multi-layered defenses by implementing measures such as virtual patching[6]—e.g., through cloud-based Web Application Firewalls (WAFs), which can deliver timely effects—as well as introducing bot mitigation measures. In addition, financial institutions should enhance protections against lateral movement following an intrusion, including through network segmentation, multi-factor authentication for privileged accounts, and improved detection capabilities such as Endpoint Detection and Response (EDR).

These measures are intended to mitigate risk and do not eliminate it. Financial institutions should therefore assess residual risks and follow appropriate risk acceptance procedures where necessary.

(8) Preparation for the Disruption of Priority Services and IT Systems

[6] A virtual patch is a temporary solution used when it is difficult to promptly apply vendor-provided security patches to servers or other systems. It involves deploying devices equipped with intrusion prevention rules tailored to specific vulnerabilities along network paths, thereby blocking malicious traffic that exploits those vulnerabilities. However, it should be noted that such measures are not permanent solutions, as they can only protect traffic passing through those network paths and may not be able to keep pace with evolving variants of attack code.

On the premise that cyberattacks cannot be completely prevented even with comprehensive measures, top executives should plan for scenarios in which service and IT systems may be disrupted by cyberattacks and consider, as a contingency option, the proactive suspension of the priority services and IT systems identified in (2).

In preparation for such scenarios, it is important to assess the effectiveness of business continuity plans (BCPs), the adequacy of procedures for responding to customers and other stakeholders, and emergency communication frameworks, and to clearly establish internal criteria and procedures for the proactive suspension of services and IT systems in the event of heightened cyber risk. These considerations apply equally to systems operated under joint arrangements or provided by cloud service providers.

Top executives should also recognize that shortening patching timelines by reducing testing, as described in (6), may increase the frequency of IT system failures due to insufficient testing.

Furthermore, financial institutions should be prepared for scenarios in which, not only in internally developed and maintained IT systems but also in third-party software and services, the identification of critical vulnerabilities may necessitate the disruption of their use or the discontinuation of such services.

(9) Maintaining and Strengthening External Collaboration

Given that a large volume of information on frontier AI is released in a short period of time, it is difficult for individual institutions to comprehensively capture all developments on their own. Accordingly, they should actively collect information from sources such as Financials ISAC Japan, industry groups and communities, and regulatory authorities.

In addition, in responding to frontier AI, financial institutions should actively share their practices within mutual-assistance communities, such as Financials ISAC Japan, thereby contributing to enhancing the resilience of the financial sector.