Resources on Frontier AI and Cybersecurity

As of September 2, 2026

The Federal Reserve has compiled resources on this page that may be helpful to institutions as they manage the opportunities and risks of frontier artificial intelligence (AI) for cybersecurity.[1] These resources on frontier AI were developed by organizations external to the Federal Reserve based on their experience using and/or researching frontier AI models.

This page also includes resources to promote fundamental cyber hygiene practices. The application of basic cyber hygiene practices is essential to defending against a wide range of cyber risks. This includes such practices as timely updating and patching of systems, network segmentation, access control based on the principle of least privilege, end user training, and event detection and logging.

This is a voluntary resource providing a non-exclusive compilation of publicly available content on websites external to the Federal Reserve for convenience and informational purposes only. These external websites may contain content that is copyrighted with restrictions on reuse and permission to use those materials must be obtained from the website owner. The Federal Reserve is not responsible for the content of these websites. The Federal Reserve neither endorses the information, content, presentation, or accuracy nor makes any warranty of any kind, expressed or implied, regarding the linked websites or the organizations sponsoring the linked websites and does not endorse the views expressed or the products/services offered. This resource does not have the force or effect of law and does not prescribe any specific practices or standards nor establish any safe harbors for compliance with laws or regulations. Organizations with questions or who wish to share resources through this site may contact supervision@stls.frb.org.

Resources on General Cyber Hygiene

Federal Reserve Board

- Cybersecurity Resources for Community Banks

Other Government Agencies

- National Institute of Standards and Technology (NIST) – Cybersecurity Framework
- Cybersecurity and Infrastructure Security Agency (CISA) – Cross-Sector Cybersecurity Performance Goals
- CISA – Cyber Hygiene Services
- CISA Vulnerability Review FY 2024/2025

[1] Frontier AI generally include Large Language Models (LLM) that are the most advanced at any given moment, representing the leading edge of AI capability. These capabilities include rapidly identifying vulnerabilities and, in some cases, aiding in the development of methods to exploit those vulnerabilities.

Industry Organizations

- Cyber Risk Institute (CRI) – CRI Profile
- Center for Internet Security (CIS) – Critical Security Controls

Conference of State Bank Supervisors

- Conference of State Bank Supervisors (CSBS) – The Fundamentals of Cyber Hygiene for Financial Institutions

Resources on Frontier AI

Government

- CISA – Five Eyes Cyber Security Agencies Statement

Industry Organizations

- Financial Services Information Sharing and Analysis Center (FS-ISAC) – Sector Risk Advisory: Preparing the Enterprise for AI-Enabled Vulnerability Discovery
- American Bankers Association (ABA) – AI-Assisted Vulnerability Detection & Remediation: Assessment Questions for Core Service Providers
- Independent Community Bankers of America (ICBA) – Community Banker Guide on Artificial Intelligence Security Readiness
- Cloud Security Alliance (CSA) – The AI "Vulnerability Storm": Building a "Mythos-Ready" Security Program

Individual Banks and Service Providers

- JPMorganChase – Fortifying the enterprise: 10 actions to take now for AI-ready cyber resilience
- Visa – Frontier AI: A New Era of Cyber Resilience
- FISERV – Cybersecurity Best Practices in a Rapidly Evolving Threat Environment