Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

March 15, 2025

To: Networking and Information Technology Research and Development (NITRD), National Coordination Office (NCO), and National Science Foundation (NSF)

Sent: Via email to ostp-ai-rfi@nitrd.gov

Subject: AI Action Plan: Comments from Financial Services Sector Coordinating Council

The United States stands at a pivotal moment in Artificial Intelligence (AI) innovation, particularly within the financial sector. As financial institutions continue to integrate and scale AI across their technology applications, including for fraud detection, cybersecurity, underwriting, and customer service, it is imperative to keep managing the risks these technologies pose to the financial system, as well as its clients and customers. In parallel, adversaries are leveraging AI to enhance cyberattacks and fraud, posing new threats to financial institutions that could undermine financial stability.

The Financial Services Sector Coordinating Council (FSSCC) is an industry-led, nonprofit established in 2002 to coordinate critical infrastructure protection across the financial services industry. Our diverse membership includes financial institutions of all types and sizes—from community banks and credit unions to insurance companies, financial utilities and trade associations— representing the breadth of the sector.

We applaud the Trump Administration's commitment to bolstering American leadership in AI and its emphasis on innovation and economic growth. Members of the FSSCC believe that sustaining leadership in AI necessitates a balanced approach—one that prioritizes cybersecurity and strong governance alongside technology advancements. In this response, we outline several specific policy actions, as requested in the RFI, to secure AI-driven financial services and further the United States' global leadership in technology and finance.

To achieve these goals, we recommend that policymakers take the following actions:

1. **Establish AI Security Standards:** Through the National Institute of Standards and Technology (NIST), establish comprehensive AI-specific cybersecurity standards that align with existing NIST frameworks, such as the Cybersecurity Framework, Privacy Framework, and AI Risk Management Framework. These standards will help financial institutions to design and deploy AI systems with robust safeguards against cyber threats and adversarial manipulation, while also facilitating integration and promoting adoption. By creating voluntary cybersecurity standards for AI, participants from both the public and private sectors can reduce vulnerabilities, protect consumers, and build trust in AI-driven tools used in the financial sector.
2. **Strengthen Collaboration on AI Standards:** Promote stronger collaboration between government, industry, and international standard-setting bodies in the development of AI cybersecurity standards. A coordinated approach will align AI standards across different jurisdictions and prevent a fragmented regulatory environment. Encourage organizations like NIST to continue their workshops and active participation in international standards-setting bodies. Enhanced cooperation will accelerate the adoption of best practices for AI security and reliability across the financial sector.

3. **Share Intelligence on AI-Enabled Threats:** Improve the sharing of threat intelligence related to AI-enabled attacks and fraud through collaboration with industry-specific information-sharing hubs and the Sector Risk Management Agencies (SRMAs). In the financial sector, regulators and security agencies should work with information-sharing hubs like the Financial Services Information Sharing and Analysis Center (FS-ISAC) to exchange timely insights on emerging AI-driven threats, including AI-generated phishing scams and deepfake fraud. Strengthen cross-sector communications, such as those facilitated through the Department of Homeland Security (DHS), to share threat intelligence, attack patterns, and mitigation strategies. These efforts further help the financial sector proactively defend against AI-enabled threats and enhance the resilience of critical infrastructure.
4. **Enhance Digital Identity Ecosystem**: Collaborate with industry to develop effective training practices for recognizing and mitigating AI-based fraud tactics. Identify actions for U.S. and state governments to take to bridge the gap between physical and digital government credentials. Enable validation of identity information against government "reservoirs of truth" to ensure safe, secure, privacy-preserving, and reliable transactions. Improve financial institutions' ability to trust and digitally validate government ID documents and other digital attributes during enrollment and authentication processes.
5. **Support Broader Adoption of Fraud Prevention Measures:** Explore ways to reduce cost barriers for smaller financial institutions by offering public services that enhance access to AI-driven fraud detection and advanced deepfake detection tools that will aid smaller entities to adopt necessary protections without financial burden and strengthen the overall security and integrity of the financial system.

The Trump Administration has a unique opportunity to solidify American leadership in AI-driven financial services by promoting innovation, enhancing security through robust safeguards, and fostering strategic collaboration. By implementing these policy recommendations, the administration can enhance the resilience of the U.S. financial sector, deter adversarial threats, and drive economic growth, thereby securing America's technological and economic future while protecting the stability of our financial system.

The FSSCC appreciates the opportunity to respond to this RFI and your consideration of our recommendations. We welcome further dialogue on these proposals and other critical issues affecting the security and resilience of the financial sector.

Deborah Guild
FSSCC Chair
Executive Vice President and Head of Technology, PNC Financial Services