Chairman Jay Obernolte

Promoting Advanced Artificial Intelligence Innovation and Security

Administration Policy:

On June 2, 2026, the White House issued an executive order (EO) to promote advanced artificial intelligence innovation and security. The EO directs federal agencies to rapidly develop cybersecurity standards and evaluation frameworks for advanced AI systems while simultaneously bolstering America's cyber defenses across national security, defense, and civilian government networks.

The EO makes it the policy of the United States to promote AI innovation and security, modernize information systems, strengthen cybersecurity defenses against external threats, protect American intellectual property and technological advantages from foreign adversaries, and expand advanced AI-enabled capabilities.

The EO directs the Committee on National Security Systems to prioritize the cyber defense of national security systems within 30 days. It also requires the Secretary of War to prioritize cybersecurity protections for Department of War information systems and authorizes the Secretary of Homeland Security to issue directives and guidance to expand federal cybersecurity programs utilizing AI-enabled defensive tools. The EO further directs federal agencies to increase access to cybersecurity tools and services for state and local governments as well as critical infrastructure operators, such as rural hospitals, community banks, and local utilities.

Additionally, the EO instructs the Secretary of the Treasury to establish an AI cybersecurity clearinghouse that will work with the AI industry and infrastructure operators on a voluntary basis to discover and validate software vulnerabilities, prioritize remediation efforts, and coordinate distribution of security patches.

The EO also establishes a classified benchmarking process to evaluate the advanced cyber capabilities of AI models and determine when a system qualifies as a "covered frontier model." The EO creates a voluntary framework for AI developers to engage with the federal government on model classification, limited pre-release security access, and selection of trusted early-access partners, while explicitly stating that no mandatory licensing or preclearance regime is created.

Background:

- The EO will provide the federal government with an "early look" at certain powerful AI models to increase the government's awareness of potential security risks.
- According to Office of the Director of National Intelligence guidance, frontier AI models "refer to any general-purpose AI system near the cutting-edge of performance, as measured by widely accepted publicly available benchmarks, or similar assessments of reasoning, science, and overall capabilities."
- According to the World Economic Forum, new frontier AI models may introduce new cybersecurity risks as they can autonomously identify previously unknown vulnerabilities, generate working exploits, and carry out complex cyber operations with minimal human input.
- The Committee on National Security Systems was established in 1990 under National Security Directive 42 (NSD-42) and is an interagency body charged with handling national security information by all national security systems. National security systems are defined under 44 U.S.C. § 3552(b)(6) as any information system operated by or on behalf of the federal government that involves intelligence activities, cryptologic activities related to national security, command and control of military forces, or equipment that is an integral part of a weapon or weapon system.