EXECUTIVE ORDER

- - - - - - -

PROMOTING ADVANCED ARTIFICIAL INTELLIGENCE
INNOVATION AND SECURITY

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Sec. 1. Purpose. The United States continues to lead the world in Artificial Intelligence (AI) because of the enormous talent and innovation of our AI industry, and because we refuse to stifle this innovation with overly burdensome regulation. My Administration has unleashed tremendous technological growth and economic investment in AI by slashing the bureaucratic constraints that the prior Administration placed on America's AI developers and researchers, and by instead encouraging AI innovation and accelerating responsible AI adoption across government and industry.

Advanced AI capabilities make our Nation stronger, but also introduce new national security considerations that require coordinated action across executive departments, agencies, and components. As these capabilities evolve, my Administration will continue to work closely with industry to ensure that the best and most secure technology is deployed rapidly to confront any and all threats to our country. We will continue to lead an America First cybersecurity effort that enhances both our

national security and our global AI dominance.

It is the policy of the United States to promote AI innovation and security by working collaboratively with the private sector to modernize government and private sector information systems and harden them against external threats; to protect American ingenuity and intellectual property from exploitation and theft by adversaries; and to cultivate America's advanced AI-enabled capabilities.

Sec. 2. Upgrading American Systems for Advanced AI.

(a) Within 30 days of the date of this order, the Committee on National Security Systems shall prioritize the cyber defense of National Security Systems, as defined in 44 U.S.C. 3552(b)(6)(A), by taking appropriate and expeditious action consistent with the purpose of this order.

(b) Within 30 days of the date of this order, the Secretary of War shall prioritize the cyber defense of Department of War information systems by taking appropriate and expeditious action consistent with the purpose of this order.

(c) Within 30 days of the date of this order, the Secretary of Homeland Security, through the Director of the Cybersecurity and Infrastructure Security Agency (CISA), in consultation with the Director of the Office of Management and Budget (OMB), the Assistant to the President for National Security Affairs, and the National Cyber Director, shall release

Binding Operational Directives and other guidance as appropriate to:

(i) expedite and prioritize the cyber defense of civilian Federal Government information systems in order to protect our Nation's vital functions;

(ii) establish or expand Federal programs and cybersecurity services that enhance AI-enabled defensive tools; and

(iii) facilitate access to cybersecurity tools and services including, where appropriate, covered frontier models for Federal agencies, State and local authorities, and operators of critical infrastructure such as rural hospitals, community banks, and local utilities.

(d) Within 30 days of the date of this order, the Secretary of the Treasury, in consultation with the National Cyber Director, the Secretary of War, through the Director of the National Security Agency (NSA), and the Secretary of Homeland Security, through the Director of CISA, shall form an AI cybersecurity clearinghouse, in voluntary collaboration with the AI industry and operators of critical infrastructure, that coordinates and deconflicts scanning for software vulnerabilities, discovers and validates such vulnerabilities, and coordinates and prioritizes remediation and distribution of vulnerability patches.

(e) Within 30 days of the date of this order, the Director of OMB, in coordination with the National Cyber Director and the Director of CISA, shall determine whether any Federal grant programs have available and relevant funding that can be directed toward applicants developing advanced AI vulnerability detection.

(f) Within 60 days of the date of this order, the Director of the Office of Personnel Management shall expand the U.S. Tech Force Information Cybersecurity Specialist hiring and placement pathways.

Sec. 3. Secure Frontier Model Deployment. Within 60 days of the date of this order, the Secretary of the Treasury, the Secretary of War, through the Director of NSA, and the Secretary of Homeland Security, through the Director of CISA, in consultation with the White House Chief of Staff, through the National Cyber Director, the Assistant to the President for Science and Technology (APST), and the Director of the National Institute of Standards and Technology, and in coordination with other executive departments and agencies, as appropriate, shall:

(a) develop and maintain a classified benchmarking process to assess the advanced cyber capabilities of AI models and determine the threshold at which an AI model should be designated a "covered frontier model" for the purposes of this order, sharing such assessments with AI developers and

researchers as appropriate. Such a determination shall be made by the Director of NSA, in consultation with the National Cyber Director, the APST, the Director of CISA, and other representatives of the Department of War, as appropriate.

(b) design a voluntary framework with AI developers through which developers would be able to:

(i)engage the U.S. Government to determine whether model(s) under development meet the designation of "covered frontier model";

(ii)provide the Federal Government with access to covered frontier models, subject to appropriate confidentiality, cybersecurity, insider-risk, and intellectual-property protection, use, and nondisclosure requirements, for a period of up to 90 days before they plan to release such models to other trusted partners; and

(ii) collaborate with the Federal Government to select trusted partners that will have early access to covered frontier models to promote secure innovation and strengthen the cybersecurity of critical infrastructure.

(c) Nothing in this section shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models.

Sec. 4. Protection Against Criminal Actors. The Attorney General shall prioritize the enforcement of 18 U.S.C. 1028, 18 U.S.C. 1030, 18 U.S.C. 1343, and all other applicable Federal criminal laws against anyone who utilizes AI to illegally access or damage a computer without authorization, or who utilizes AI while engaged in such illegal access to further any other crime. This includes breaching any public or private information technology system, or employing AI agents to unlawfully access data or information that is subsequently used for a criminal or unlawful purpose.

Sec. 5. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(d) The costs of publication of this order shall be borne by the Department of War.

THE WHITE HOUSE

May XX, 2026.