COMMONWEALTH of VIRGINIA

Executive Department

EXECUTIVE DIRECTIVE 6 (2026)

DIRECTING A COMMONWEALTH-WIDE PREPAREDNESS APPROACH TO CYBER THREATS POSED BY ARTIFICIAL INTELLIGENCE AND RECURSIVE SELF-IMPROVEMENT DEVELOPMENT

In Executive Order No. 19 (2026), I directed the Secretary of Public Safety and Homeland Security to establish the Virginia Unified Readiness Framework as the Commonwealth's enterprise-wide governance model for all-hazards preparedness and resilience. The hazards covered by Executive Order No. 19 include cybersecurity threats, cyber incidents, and threats to critical infrastructure.

In Executive Order No. 22 (2026), I directed the formation of the rapid-response AI Task Force ("AI Task Force") to address the unprecedented risks facing the Commonwealth from unregulated artificial intelligence ("AI") development. The AI Task Force, in coordination with the Secretary of Public Safety and Homeland Security, has identified substantial and growing cybersecurity risks from AI development, including biorisk and physical infrastructure risks to the Commonwealth's critical systems, and determined that immediate action must be taken to ensure robust processes are in place to protect all Virginians.

Accordingly, by virtue of the authority vested in me as Governor under Article V of the Constitution of Virginia and §§ 2.2-222.1 and 44-146.16 to 44-146.18 of the *Code of Virginia*, I hereby direct the preparation of a coordinated cyber threat response and infrastructure-hardening plan for the Commonwealth under the Unified Readiness Framework that accounts for the risks and mitigates the hazards posed by existing AI models, and the prospect of threat amplification from recursive self-improvement AI development. As part of the Unified Readiness preparedness process, the AI Task Force shall seek input and participation from the AI frontier model developers and other public and private sector participants in order to access and learn from information that has been or may be shared with other governmental actors about the risks posed by existing AI models and new models under development, as well as recursive self-improvement AI development, and to otherwise identify recommended best practices for guarding against AI-based cyber threats.

Importance of the Issue

The acceleration of AI development presents significant, unprecedented risks as reflected by the calls from major AI technology companies to slow down the pace of development. Virginia's Unified Readiness Framework exists to address dynamic and complex threats that demand a modern integrated approach to preparedness. Preparing now for constantly evolving AI risks is critical to the safety and security of Virginia and its residents. The Commonwealth

expects that leading AI technology companies—who rely on Virginia-based compute, provide their services to Virginians, and are directly soliciting government engagement—will collaborate to explain the current and foreseeable issues and risks with today's publicly available models as well as internal models, and work in partnership on preparedness to protect critical systems and infrastructure on which everyone in the Commonwealth relies.

A leading cause for concern today is recursive self-improvement AI development, which generally refers to how frontier AI models can improve themselves and build the next version of the AI model. There are different levels of recursive self-improvement AI development, ranging from a person guiding an existing AI model on the development of a future, higher capacity AI model to an AI model working fully autonomously to build and train a future AI model. All versions of recursive self-improvement AI development, however, result in the faster creation of newer, more intelligent AI models.

Although AI development has the potential for societal benefits, those benefits cannot come at the expense of responsible growth and development that ensures the safety and security of people. Chief Executive Officers at frontier AI technology companies have made clear that there are significant safety and security risks associated with models being tested today that they project will worsen with recursive self-improvement AI development. Virginia must take the concerns of the businesses leading these development processes seriously.

Directive

Pursuant to the authority vested in me as the Chief Executive Officer of the Commonwealth, I hereby direct the Secretary of Public Safety and Homeland Security and the AI Task Force take the following immediate steps to address the cybersecurity risks associated with existing AI models and recursive self-improvement AI development:

1. The Secretary of Public Safety and Homeland Security shall establish a Cyber Consortium and integrate AI-related cybersecurity as part of the Unified Readiness Framework to ensure the Commonwealth is prepared in the event of an AI-related cyber-attack.

    a. The Cyber Consortium, as part of its integration into the Unified Readiness Framework, shall adopt a Commonwealth-wide cyber-attack prevention and response plan as well as an infrastructure-hardening plan that addresses AI-related risks and other identified cyber risks. The Secretary shall review and incorporate any existing plans, projects, or assessments that bolster preparedness, where appropriate. The Secretary may, in his discretion and in coordination with the AI Task Force, direct the Cyber Consortium to conduct an independent cyber readiness review.

    b. The Secretary shall directly coordinate with all agencies within the Secretariat, including but not limited to the Virginia State Police and the Virginia Department of Emergency Management, and engage with the AI Task Force and the Chief Information Officer at the Virginia Information Technology Agency. All other executive branch agencies shall cooperate with the Secretary upon request.

c. The Secretary, in consultation with relevant Secretariats, shall designate executive branch agencies who will participate in the Cyber Consortium on an active and ongoing basis as part of the Unified Readiness Framework.

2. The AI Task Force shall engage with the leading AI technology companies, researchers, other government officials and regulators—including international experts and authorities—and private sector leaders to seek their ongoing participation and engagement with the Cyber Consortium and in the development of the Unified Readiness Framework and response plans as it relates to existing AI-related risks and future risks attributable to ongoing AI model development including hacks, biorisk, physical infrastructure risk, and recursive self-improvement development.

   a. Where applicable, AI technology companies shall be specifically requested to provide confidential briefings and reports that are submitted to other government actors—including New York's Department of Financial Services under the RAISE Act and the European AI Office under the General-Purpose AI Code of Conduct—to the Cyber Consortium and other approved participants.

   b. In partnership with the participating AI technology companies and the AI Task Force, the Secretary of Public Safety and Homeland Security shall endeavor to hold Unified Readiness briefings on AI-related risks at least quarterly due to the rapid advancement of this general-purpose technology. Such briefings shall include a tabletop exercise at least annually.

   c. The AI Task Force shall ensure deployment of an independent privacy and security review team to identify and address any potential data security vulnerabilities across Virginia's interoperable data systems—including their associated data architecture and data governance processes—to improve system security while enhancing function

3. The AI Task Force, in coordination with the Secretary of Public Safety and Homeland Security, shall engage with the public institutions of higher education to leverage their expertise to assess AI cyber-risk preparedness and recursive self-improvement AI development.

4. The AI Task Force and Secretary of Public Safety and Homeland Security shall engage with other states and invite them to participate in the Unified Readiness Framework and preparedness briefings on a bipartisan basis. Participating states will be required to maintain the confidentiality of any highly sensitive information obtained through the Cyber Consortium or under the Unified Readiness Framework on the same terms as the Commonwealth.

5. The Secretary of Public Safety and Homeland Security shall assess any and all public-private information sharing conduits and portals related to AI risk and recursive self-improvement AI development. The Secretary shall, in coordination with the AI Task Force, seek to participate in appropriate public-private information sharing.

Effective Date of the Executive Directive

This Executive Directive shall become effective upon its signing and shall remain in full force and effect unless amended or rescinded by further executive order or directive.

Given under my hand and under the Seal of the Commonwealth of Virginia this 23rd day of October 2026.

Abigail D. Spanberger, Governor

Candi Mundon King, Secretary of the Commonwealth