Virginia Executive Directive 6 (2026)

A Commonwealth-Wide Preparedness Approach to AI-Related Cyber Threats

October 23, 2026

Overview

Governor Abigail Spanberger issued Executive Directive 6 (2026), *Directing a Commonwealth-Wide Preparedness Approach to Cyber Threats Posed by Artificial Intelligence and Recursive Self-Improvement Development*, on October 23, 2026. The directive orders preparation of a coordinated cyber threat response and infrastructure-hardening plan for the Commonwealth. It builds on two prior actions: Executive Order 19 (2026), which established the Virginia Unified Readiness Framework as the enterprise-wide governance model for all-hazards preparedness, and Executive Order 22 (2026), which formed a rapid-response AI Task Force. That Task Force, in coordination with the Secretary of Public Safety and Homeland Security, identified substantial and growing cybersecurity risks from AI development, including biorisk and physical infrastructure risk to the Commonwealth's critical systems, and determined that immediate action must be taken.

ED-6 names recursive self-improvement AI development, frontier models improving themselves and building their successors, as the central concern, citing statements from frontier AI company chief executives that the safety and security risks present in models tested today will worsen as that capability advances. The directive is issued 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and 44-146.16 to 44-146.18 of the Code of Virginia, took effect on signing, and remains in force until amended or rescinded. It assigns responsibilities and establishes a planning process; it does not itself appropriate funding or set completion deadlines.

Cyber Consortium and the Unified Readiness Framework

Directive 1 creates the Cyber Consortium and divides responsibility between the Secretary of Public Safety and Homeland Security and the Consortium itself:

- **The Secretary establishes the Cyber Consortium:** and integrates AI-related cybersecurity into the Unified Readiness Framework, so the Commonwealth is prepared in the event of an AI-related cyber-attack.
- **The Consortium adopts two plans**: a Commonwealth-wide cyber-attack prevention and response plan, and an infrastructure-hardening plan, both addressing AI-related and other identified cyber risks. The Secretary reviews and incorporates existing plans, projects, and assessments where appropriate, and may, at his discretion and in coordination with the AI Task Force, direct the Consortium to conduct an independent cyber readiness review.
- **Coordination spans the full Secretariat**: the Secretary coordinates directly with all agencies within it, including but not limited to the Virginia State Police and the Virginia Department of Emergency Management, and engages the AI Task Force and the Chief Information Officer at the Virginia Information Technology Agency. All other executive branch agencies cooperate upon request. The Secretary, in consultation with relevant Secretariats, designates which agencies participate in the Consortium on an active and ongoing basis.

AI Industry Engagement and Information Sharing

Directive 2 tasks the AI Task Force with drawing leading AI technology companies, researchers, government officials and regulators, including international authorities, and private sector leaders into the Cyber Consortium and the Unified Readiness planning process. The stated scope covers existing AI-related risks and future risks from ongoing model development, including hacks, biorisk, physical infrastructure risk, and recursive self-improvement development.

- Where applicable, AI technology companies are **requested** to provide the Cyber Consortium with confidential briefings and reports they already submit to other government actors, including New York's Department of

© 2026 Carahsoft Technology Corp. Proprietary & Confidential

Financial Services under the RAISE Act and the European AI Office under the General-Purpose AI Code of Conduct. This is a request for voluntary sharing of existing filings, not a Virginia reporting obligation.

- The Secretary, with participating AI companies and the AI Task Force, is to endeavor to hold Unified Readiness briefings at least quarterly, including a tabletop exercise at least annually.
- The AI Task Force **shall ensure deployment of an independent privacy and security review team** to identify and address data security vulnerabilities across Virginia's interoperable data systems, including their associated data architecture and data governance processes.
- Directives 3 through 5 extend engagement to Virginia's public institutions of higher education, to other states invited on a bipartisan basis under equivalent confidentiality terms, and to an assessment of existing public-private information sharing conduits and portals related to AI risk.

What Does This Mean for Government?

Execution sits with two parties: the Secretary of Public Safety and Homeland Security and the AI Task Force. Other executive branch agencies are obligated only to cooperate upon request, though the Secretary may designate them as ongoing Consortium participants.

- Two plans must be adopted; Cyber-attack prevention and response, and infrastructure hardening, each addressing AI-related risk.
- Existing preparedness work is to be reviewed and folded in rather than duplicated, which matters for agencies with assessments already underway.
- The required independent review reaches data architecture and governance processes across interoperable systems, not perimeter security alone.
- The Secretary is directed to endeavor to hold briefings at least quarterly with an annual tabletop exercise, a recurring rhythm rather than a one-time deliverable.
- Coordination reaches every agency within the Secretariat, State Police and VDEM are named as examples, not the full list — while ongoing Consortium membership is designated by the Secretary in consultation with relevant Secretariats.

The directive sets no completion deadlines and carries no appropriation, so sequencing and resourcing will be determined through the Unified Readiness Framework and the normal budget process.

What Does This Mean for Industry?

ED-6 is a planning and coordination directive, not a procurement action: it creates no contract vehicle and no funding. What it does create is a defined planning process with named owners, a recurring briefing cadence, and an explicit requirement for independent review, each of which tends to generate requirements over time.

Key takeaways for vendors:

- The independent privacy and security review team is the clearest near-term services opportunity, with scope spanning interoperable data systems, data architecture, and data governance.
- The two required plans create demand for threat modeling, incident response planning, and operational technology and critical infrastructure assessment.
- Quarterly briefings and an annual tabletop point to recurring exercise design, facilitation, and readiness measurement work.
- Public higher education is written in as an expertise partner, making university research centers both collaborators and potential channel partners.
- The multi-state invitation means positioning built for Virginia may be reusable with other states that accept, subject to confidentiality terms.

© 2026 Carahsoft Technology Corp. Proprietary & Confidential

Because ED-6 is unfunded, the practical path runs through the Secretary of Public Safety and Homeland Security, VITA, and the AI Task Force as the Unified Readiness plans take shape, and through existing Commonwealth contract vehicles rather than any new mechanism.

Timeline

Policy	Key Dates	Focus & Key Provisions
EO 19 (2026): Virginia Unified Readiness Framework	**2026**	Established the Commonwealth's enterprise-wide governance model for all-hazards preparedness and resilience. Covered hazards include cybersecurity threats, cyber incidents, and threats to critical infrastructure.
EO 22 (2026): Rapid-Response AI Task Force	**2026**	Formed the AI Task Force to address risks from unregulated AI development. The Task Force, in coordination with the Secretary of Public Safety and Homeland Security, identified growing cybersecurity, biorisk, and physical infrastructure risks to Commonwealth systems.
ED-6 (2026): AI Cyber Threat Preparedness	**Oct 23, 2026**	Directs a coordinated cyber threat response and infrastructure-hardening plan under the Unified Readiness Framework and establishes the Cyber Consortium. Effective on signing.
Cyber Consortium formation	**Not specified**	Secretary of Public Safety and Homeland Security establishes the Consortium and designates participating agencies in consultation with relevant Secretariats. No deadline is set.
Unified Readiness AI briefings	**At least quarterly**	Secretary shall endeavor to hold briefings on AI-related risks with participating AI companies and the AI Task Force, including a tabletop exercise at least annually.
Independent privacy and security review	**Not specified**	AI Task Force deploys an independent review team across Virginia's interoperable data systems, data architecture, and data governance processes.
NY RAISE Act / EU GPAI Code of Conduct	**Ongoing**	External regimes under which AI companies already file confidential reports. ED-6 requests those filings be shared with the Cyber Consortium where applicable.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.

© 2026 Carahsoft Technology Corp. Proprietary & Confidential