ASPEN POLICY ACADEMY
aspen institute

Securing Virginia's Operational Technology from Cyberattacks

November 2026

Christian Crumlish
Guillermo Fisher
Colin Jenkel
Nick Kotakis

To learn more about this project, visit aspenpolicyacademy.org. Please note that all authors' opinions published here are their own. This publication does not reflect the views of the Aspen Policy Academy or the Aspen Institute.

Executive Summary

This project recommends that the Commonwealth of Virginia expand its operational technology (OT) security certification to better protect Virginia's computerized systems against growing cyber threats. State OT systems – the computer systems that run physical processes like water treatment and traffic signals – are uniquely vulnerable to threats. The rapid development of new artificial intelligence (AI) models has enabled bad actors to more easily hack into these systems, putting these computer-operated government infrastructures at risk. By expanding its existing OT security model and centralizing its security efforts across the state, this proposal would protect the systems Virginians rely on daily and set an example for other states looking to strengthen their OT cybersecurity.

Problem

Advanced AI models have made it easier for bad actors to hack into state OT, posing a threat to the critical government infrastructure that runs on these systems. Cyberattacks on the OT behind US water systems have risen sharply. In July 2026 alone, the Cybersecurity and Infrastructure Security Agency confirmed that more than over 100 internet-exposed water systems were targeted across 12 states. Importantly, state OT systems manage critical government infrastructure essential to everyday life such as water treatment and traffic signals, meaning these computerized systems shape residents' daily lives and cannot simply be turned off when security concerns arise. While Virginia has taken steps to set security standards for state agencies, each agency decides for itself whether to apply them to its OT. Virginia also lacks clear visibility into OT systems used across state agencies and their vulnerability to cyberattacks.

Solution

This project proposes that the Commonwealth of Virginia expand its existing OT security certification and centralize security efforts across state systems. In particular, this project recommends that Virginia adopt 5 key actions: 1) certifying all state-owned OT against the State's baseline security standard, 2) reprioritizing part of Virginia's cybersecurity grant funding toward securing OT, 3) adopting a containment-focused OT strategy based on federal guidance, 4) exploring ways to support privately operated OT, and 5) identifying a Commonwealth official to manage these new efforts. Together, these steps would help defend these critical computerized systems from cyberattacks, ultimately protecting Virginians from bad actors and securing the public goods and systems they rely on.

> *"Adopting these 5 recommendations would make Virginia safer and improve its cybersecurity posture by shifting the Commonwealth from a reactive strategy of chasing vulnerabilities to a proactive strategy of containment."*
>
> **Christian Crumlish, Guillermo Fisher, Colin Jenkel, and Nick Kotakis**

If you'd like to learn more, see the full project at aspenpolicyacademy.org/project/virginia-operational-systems-cybersecurity-2026.

ASPEN POLICY ACADEMY
aspen institute

aspen institute

About the Aspen Policy Academy

The Aspen Institute's Policy Academy helps community leaders and experts across the political spectrum elevate their voices, influence key decisions, and strengthen democracy from the ground up. Our innovative training programs and resources equip people across sectors – from tech to the environment, science to civic engagement – with the skills to shape critical policy efforts. Learn more at aspenpolicyacademy.org.

Header photo by BlackJack3D via Getty Images