ASPEN POLICY ACADEMY
aspen institute

Policy Brief

Extending Virginia's Proven Operational Technology Security Model Across the State

By Christian Crumlish, Guillermo Fisher, Colin Jenkel, and Nick Kotakis
November 2026



This policy project was developed by Aspen Policy Academy alumni. They worked with the Commonwealth of Virginia to propose a way to better protect its systems against cyber threats enabled by frontier AI models. This policy brief provides an overview of the alumni's proposed solution. The full project is available here. 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

Given the threat posed by advanced artificial intelligence models that are making it easier to target operational technology (OT) systems – computer systems that run physical processes like water treatment, traffic management, and state facilities – the Commonwealth of Virginia should expand OT security certification and centralize security efforts across state systems. The Virginia Department of Transportation already certifies its internet-connected OT against the Commonwealth's baseline security standard, known as SEC530, before bringing new devices online. Virginia should expand the use of this practice by taking 5 key actions:

1. Direct all state agencies that operate connected OT to certify it against SEC530 before deployment;
2. Reprioritize a portion of Virginia's existing federal cybersecurity grant funding toward OT;
3. Adopt a cybersecurity strategy for Virginia's OT that is modeled on existing federal guidance, which emphasizes containment;
4. Explore a parallel mechanism to support security coverage for privately operated critical OT infrastructure in Virginia; and
5. Name one accountable official to lead the effort across agencies.

Background

Operational technology (OT) is the set of computerized systems that run physical processes: the controls behind water treatment, traffic signals, and power and building systems in state facilities. Unlike email or databases, these systems cannot simply be taken offline and patched on a vendor's schedule without interrupting the services they deliver.

That makes them hard to fix quickly, and attackers have noticed. On July 26 and 27, 2026, a coordinated attack hit more than 30 community water systems in Minnesota, most of them small municipal utilities with little cybersecurity staff. It did not stop there: By late August, the federal Cybersecurity and Infrastructure Security Agency (CISA) confirmed that more than 100 water systems reachable and controllable through the public internet had been targeted in July alone across at least 12 states. Advanced artificial intelligence models, sometimes called "frontier" models, are making this situation worse by lowering the cost and skill needed to find and exploit these weaknesses. Virginia's Department of Health issued a drinking water cybersecurity advisory on July 29, 2026. The systems now under attack elsewhere are the same kinds of systems that Virginia's security coverage does not yet fully reach.

Virginia has taken real steps to secure its OT. Its cybersecurity statute (Code of Virginia § 2.2-2009) directs the Virginia Information Technologies Agency to set security standards for state agencies through its Information Security Standard, known as SEC530. This standard reaches the networks that these systems use to communicate, though not the physical machinery itself. Agencies decide for themselves whether to apply it to their OT; it is not required statewide. The Virginia Department of Transportation (VDOT) has established the Operations Technology Critical Infrastructure certification program to evaluate connected operations technology field devices against VDOT and Commonwealth of Virginia cybersecurity specifications and requirements. Aside from VDOT, it is unclear how widely this practice extends across other state agencies.

Despite these efforts, the Commonwealth lacks centralized visibility into the OT that exists across state agencies and which systems are exposed to the public internet and therefore vulnerable to cyberattacks. Virginia's 2020 legislative study (House Joint Resolution 64) found that cybersecurity maturity across localities varied widely and that the Commonwealth is often not informed when an organization is compromised.

Localities can draw on the federal State and Local Cybersecurity Grant Program (SLCGP), which funds cybersecurity work for local governments and which the US Environmental Protection Agency actively promotes to municipal water systems. While the federal grant program already permits OT spending, Virginia cannot take advantage of it because the Commonwealth's current Cybersecurity Plan does not include it. The plan's 5 approved objectives focus exclusively on information technology assets such as endpoints, email filtering, and vulnerability scanning.

Current federal guidance from CISA (the CI Fortify framework) and guidance from the National Institute of Standards and Technology (NIST) emphasizes a containment approach to securing OT, which is the ability to quickly isolate a compromised system from other networks, including the internet, so that an attack cannot spread while essential services keep running.

Recommendation

Virginia should extend the OT security model that it already uses inside the state government rather than build something new. Virginia can do so by taking 5 actions, all achievable under existing authority:

1. **Certify state-owned operational technology.** Direct state agencies that run connected OT to check those devices against the state's existing security standard (SEC530) before connecting them to the network, using the Virginia Department of Transportation's practice as the model.

2. **Reprioritize a portion of grant funding toward operational technology.** Update the Commonwealth's cybersecurity plan and direct an appropriate share of the state's federal cybersecurity grant funding toward OT, alongside the information technology work it already supports.

3. **Adopt a cybersecurity strategy for Virginia's operational technology that is modeled on existing federal guidance, which emphasizes containment.** Using federal guidance from CISA and NIST, the Commonwealth could develop a cybersecurity plan and issue its own guidance on how a containment strategy could be applied to OT in the state. Virginia could develop a containment approach through a few straightforward steps: identifying the systems essential to public service, mapping their internet connections, establishing predetermined "circuit breakers," and practicing how to safely isolate systems using offline, printed response plans.

4. **Explore a parallel mechanism to support security coverage for privately operated critical operational technology infrastructure in Virginia.** Use the convening authority of the State Corporation Commission (SCC) to request that Virginia's 13 electric cooperatives report on their OT security posture and federal program participation. The state should also explore longer-term ways to support privately operated critical infrastructure that falls outside current federal funding.

5. **Name one accountable owner.** Create a dedicated OT resilience leader to drive this work across agencies. The lead should report to the state's chief information officer and coordinate closely with the chief information security officer.

Implementation Details

To implement the 5 recommended actions, Virginia can take the following steps:

1. **Certify state-owned operational technology.** The Commonwealth should explicitly direct all executive branch agencies to adopt VDOT's model, certifying internet-connected OT against the state's existing SEC530 security standard before it is allowed to touch the network. Because these systems control physical processes like water treatment and traffic, a breach carries immediate physical consequences; checking a device before it is connected keeps known vulnerabilities off the network from the start. This requires no new statutory authority and could be issued as an administrative directive today. While SEC530 was originally written for information technology and will ultimately need to be updated to explicitly address OT, applying its network-level controls today would establish an immediate, proven baseline for containment. It is a pragmatic starting point that would protect systems now while the standard matures over time.

2. **Reprioritize a portion of federal grant funding toward operational technology.** Virginia should steer an appropriate share of its federal cybersecurity grant funding toward the areas where risk is currently concentrated: municipal water and wastewater systems. By adding OT-specific objectives to the Virginia Cybersecurity Plan, the state could unlock existing SLCGP funds to help under-resourced local governments protect their OT for the first time.

3. **Adopt a cybersecurity strategy for Virginia's operational technology that is modeled on existing federal guidance, which emphasizes containment.** For critical service systems, Virginia should require operators to identify the systems needed to keep each service running; map and document how those systems connect to corporate, internet-facing, cloud, and vendor networks; establish predetermined "circuit breaker" isolation points with offline, printed response plans; and regularly test their ability to isolate affected systems. Containment works regardless of the speed of an attack, because it does not depend on patching a flaw before an attacker reaches it. It is also mostly governance and process rather than new technology, so Virginia could put this in place quickly and largely within existing budgets.

4. **Explore a parallel mechanism to support security coverage for privately operated critical operational technology infrastructure in Virginia.** Virginia should request that its 13 electric cooperatives self-report their participation in US Department of Energy cybersecurity programs and their OT posture, using the SCC's existing convening authority under the Senate Bill 1239 model. Unlike municipal water systems, private critical infrastructure operators – including electric cooperatives – are categorically excluded from federal SLCGP grant funding, and no Virginia general fund cybersecurity program currently exists to assist them. In parallel with SCC self-disclosure, the Commonwealth should evaluate longer-term mechanisms – whether through legislation, new interpretations of state funding rules, or shared services – to support privately operated critical infrastructure that carries physical consequences for Virginians but sits outside current federal aid.

5. **Name a single accountable owner.** Finally, Virginia should create a dedicated OT resilience leader to own this effort end to end. This ideally should be a distinct role, not an added duty for an existing office, which would signal that OT security is its own discipline rather than a subset of information technology security. The work cuts across agencies, including the Virginia Information Technologies Agency, Department of Transportation, Department of Health, Cybersecurity Planning Committee, and other agencies, and no existing role sits above all of them. The lead should report to the state's chief information officer, coordinate closely with the chief information security officer, and hold accountability that spans these agencies rather than sitting inside any one of them.

The implementation of these recommendations, as well as a recommended sequence and timeline for the Commonwealth, is provided in a companion roadmap. 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 — ensuring the systems that deliver critical physical services remain protected and operational regardless of how the threat landscape evolves.

If you'd like to learn more, see the full project, including a Year 1 Roadmap, an OT jurisdiction and authority map, and a comparison document for Virginia's peer states, at aspenpolicyacademy.org/project/virginia-operational-systems-cybersecurity-2026.

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