ASPEN POLICY ACADEMY
aspen institute

Roadmap

Year 1 Roadmap: Extending Operational Technology Security in Virginia

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

November 2026

This roadmap 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 roadmap offers a quarter-by-quarter guide for how the Commonwealth should secure operational technology. The full project, including a policy brief explaining the alumni's core recommendations, 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.

About This Roadmap

To help secure operational technology (OT) in the Commonwealth, Virginia should follow the Year 1 Roadmap — a quarter-by-quarter sequence for the first 12 months using existing authority. In brief, the Commonwealth should take the following 5 actions:

1. Name a leader within the government to oversee OT practices.
2. Inventory internet-connected OT across state agencies and apply a certification requirement modeled on that used by the Virginia Department of Transportation.
3. Add OT objectives and guidance to its state cybersecurity plan and steer a portion of existing grant funding toward security practices for OT.
4. Adopt security practices for OT emphasizing containment practices that are based on existing federal guidance.
5. Open an extension path for providing security coverage to localities and private operators, with the mechanism to be chosen by the Commonwealth.

The decisions that matter most, whether to deepen the work, broaden it to other sectors, or seek new authority for the cooperative and private utility gap, should be driven by the lessons learned from the first year's inventory and self-reporting.

Months 1–3: See where Virginia has full authority over its operational technology

- The chief information officer (CIO) at the Virginia Information Technologies Agency (VITA) designates the OT resilience lead. This gives the effort a single accountable owner from day 1, before any directive goes out. It is an administrative designation rather than a new statutory office.
- On the lead's recommendation, the CIO issues a directive requiring every executive branch agency to inventory its internet-connected OT. No legislation or new funding is needed. This is the single action that closes the visibility gap.
- Virginia Department of Transportation shares its Operations Technology Critical Infrastructure certification model with VITA as a template for other agencies. The practice already exists; the first step is making it available, not reinventing it.
- Identify the 5 highest consequence state owned OT systems (water treatment, traffic control, corrections, port operations, state facilities) and prioritize them for baseline assessment.
- As part of the inventory, agencies assess each high consequence OT system against the CI Fortify containment checklist developed by the federal Cybersecurity and Infrastructure Security Agency (CISA): Can we identify the minimum vital systems, have we mapped every connection, do predetermined isolation points exist, and can we rehearse full isolation?

Months 4–6: Set the standard and open the grant channel (state and locality OT)

- Coordinated by the OT resilience lead, state agencies begin certifying connected OT field devices against the Commonwealth's baseline security standard, known as SEC530, before deployment, using the VDOT model as a template. For critical service systems, certification includes a CI Fortify–aligned containment baseline: documented isolation points, offline response plans, and a tested ability to operate isolated.
- The Virginia Cybersecurity Planning Committee (VCPC) adds an OT-specific objective to the Virginia Cybersecurity Plan at its next meeting cycle. This administrative step unlocks State and Local Cybersecurity Grant Program (SLCGP) funding for locality OT projects (the federal rules already permit it; Virginia's plan just needs to point there).

- Open SLCGP Phase 3 project applications to include OT categories for localities: OT asset inventory, supervisory control and data acquisition network segmentation, and vulnerability assessment. Concurrently, the VCPC evaluates state-level mechanisms to offset the rising federal cost-share burden for qualifying rural utilities, mirroring the Clean Water Trust match model used in Massachusetts.

Months 7–9: Reach outward (locality and private/cooperative OT)

- First, SLCGP locality OT projects begin deployment, prioritizing municipally owned water and wastewater systems and rural communities (the 25% rural set-aside applies). The Office of Drinking Water's existing 2-hour operational reporting and the Fusion Center incident-reporting duty provide visibility into the projects' findings.
- Locality OT projects funded through the SLCGP align with CISA's Cross-Sector Cybersecurity Performance Goals, which cover both IT and OT and are the benchmark the federal grant program uses.
- The State Corporation Commission (SCC) sends a letter to Virginia's 13 electric cooperatives requesting disclosure of their participation in US Department of Energy cybersecurity programs (ICS-REC, RMUC, Co-op Cyber Goals) and their internet-connected OT posture. The SCC's existing convening relationship is used, creating visibility without a mandate.
- VDOT reviews cybersecurity terms in the Express Lanes Comprehensive Agreements with Transurban to assess whether current contract language addresses OT and identifies terms that could be added or amended at the next amendment window.

Months 10–12: Measure, report, and recommend year 2

- The OT resilience lead delivers the first annual report to the governor on state agency OT posture: How many systems were inventoried, how many were certified, and what gaps remain. This is the accountability mechanism, and it uses the reporting authority that the CIO already has under § 2.2-2009.
- The VCPC reports on locality OT baseline data from SLCGP assessments. This would give the Commonwealth its first statewide picture of locality OT exposure.
- The cooperative self-disclosure results inform whether year 2 should pursue voluntary shared services, incentive programs, or a legislative ask for SCC cyber authority.

- The OT resilience lead recommends year 2 scope to the governor's office: deepen (more agencies, more localities), broaden (extend to sectors like dams, 911), or legislate (if the cooperative and private utility gap requires statutory authority that the Commonwealth does not yet have).

If you'd like to learn more, see the full project, including a policy brief explaining the alumni's core recommendations, 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