ASPEN POLICY ACADEMY
aspen institute

Peer State Comparison

What Virginia's Peer States Are Already Doing on OT Cybersecurity

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

November 2026

This peer state comparison 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 peer state comparison offers examples of how 6 other states are handling operational technology (OT) cyber readiness as of fall 2026. It outlines specific programs, funding, and metrics from states that have directed resources toward OT cyber readiness for water and other critical infrastructure. 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.

A US Environmental Protection Agency enforcement review in 2024 found that roughly 70% of surveyed water systems failed to meet basic security standards, and Fortinet has reported that 1 in 3 water utilities experienced at least 1 cyber incident in the past year. Several states have responded with targeted OT funding and, in some cases, binding regulations. As of August 27, 2026, the federal Cybersecurity and Infrastructure Security Agency (CISA) confirmed that over 100 internet-exposed water systems were targeted in July 2026 alone across at least 12 states. The scope of threat actor activity has grown significantly since the initial Minnesota disclosure. The states profiled here show that this threat is being addressed using existing tools rather than waiting on new authority; each offers Virginia a concrete model to weigh against its own governance and resources.

New York: Regulation and $9 million in OT-specific grants (2026)

- In March 2026, New York announced a binding cybersecurity regulation for water utilities: Appendix 5-E to 10 NYCRR Part 5. OT cybersecurity is now part of operating a public water system, checked as part of existing sanitary surveys and inspections.

- No default credentials, complex passwords, and multifactor authentication, access limited to operational need. Larger plants (more than 10 million gallons per day) must monitor and log network activity. Operators must complete cybersecurity training for certification renewal.
- New York has backed these regulations with money with the SECURE grant program (Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements). Initially $2.5 million, boosted to $9 million in August 2026 after the multistate water attacks.
- A total of 153 local government projects funded: $50,000 grants for cybersecurity assessments, $100,000 grants for implementing upgrades.
- A former Federal Bureau of Investigation Cyber Division deputy director called New York's approach "commendable" and "a great sign and example for a lot of other states."

Key Takeaways for Virginia

New York exemplifies the most assertive path, pairing a binding regulation with dedicated state grant money so that utilities are both required to act and funded to do so. Virginia could borrow the funded-mandate pairing, but the binding regulation reaches further than the Commonwealth's current authority over locality and private water systems allows, so the grant side is the more immediately usable component.

Massachusetts: More than $2 million for small and disadvantaged water systems (2024–present)

- The Massachusetts Clean Water Trust created a state-funded OT cybersecurity grant program in 2024, targeting small and disadvantaged communities.
- The program offers grants of up to $50,000 per system for cybersecurity risk assessments and at-risk operational technology equipment.
- To date, $1.3 million has been disbursed to 38 water systems. The total commitment is at least $2 million.
- Qualifying systems are also eligible for up to $50,000 in additional State Revolving Fund grants for mitigation, so the effective cap per system is $100,000.
- According to the commissioner of the Massachusetts Department of Environmental Protection, "Water systems, particularly those in small, rural, and underserved communities, face heightened risks due to aging infrastructure and limited funding."

Key Takeaways for Virginia

Massachusetts targets its money where the need is greatest, funding cybersecurity assessments and equipment for small and disadvantaged systems through an existing state trust rather than a new program. For Virginia, it is a model for reaching the under-resourced rural utilities that a 2020 legislative study flagged and for stacking state and federal dollars to raise the effective cap per system.

Georgia: Financing explicitly for OT/industrial control system (ICS) upgrades

- The Georgia Environmental Finance Authority (GEFA) offers low-interest financing through the Drinking Water State Revolving Fund (SRF) and Clean Water SRF explicitly for cybersecurity improvements to operational technology.
- Eligible uses stated on GEFA's program page include "enhancing the security of operational technology systems," "installing or updating ICS systems," threat detection and monitoring systems, and access control.
- Projects with cybersecurity components receive additional scoring points during the pre-application evaluation, so they are more likely to be funded.
- Paired with free EPA cybersecurity assessments and CISA cyber hygiene services offered directly to utilities.

Key Takeaways for Virginia

Georgia uses financing that it already runs, adding OT and ICS upgrades as eligible uses of its revolving loan funds and giving cybersecurity projects extra scoring weight. Virginia could apply the same lever to its own revolving funds without new authority, though loans ask utilities to take on repayment, which limits their reach among the smallest systems compared with grants.

California: State and Local Cybersecurity Grant Program (SLCGP) deployed to water utility OT ($250,000 example)

- West Valley Water District received a $250,000 SLCGP grant (fiscal year 2024) administered through the California Governor's Office of Emergency Services.
- A state can use existing SLCGP funds for water utility OT cybersecurity under the current federal rules. No waiver or special authority was needed.

Key Takeaways for Virginia

California is the clearest proof of our policy brief's central point that a state can direct existing federal grant dollars to water utility OT under current rules, with no waiver or special authority. Virginia could do the same immediately; the 1 action it requires is adding an OT objective to the state's Cybersecurity Plan so that those projects become eligible.

Texas: Mandatory incident reporting of OT events and biennial assessments ($40 million SLCGP)

- Texas state law (SB 271, 88th Legislature, 2023) requires all city and county governments to report cyberattacks to the Department of Information Resources (DIR) within 48 hours; the reporting scope explicitly includes attacks in which data are not breached, covering OT disruptions like denial of service against control systems.
- State agencies must complete biennial information technology and security infrastructure assessments that include operational risk.
- DIR runs regional Security Operations Centers and provides endpoint detection and multifactor authentication services to both state and local entities.
- Texas received roughly $40 million of SLCGP funding over 3 years, among the highest state totals nationally; the 2024–2029 Texas Cybersecurity Strategic Plan explicitly addresses critical infrastructure.

Key Takeaways for Virginia

Texas leads with visibility, mandating that localities report cyberattacks, including operational technology disruptions where no data are breached, and backing it with shared state services like Security Operations Centers. Virginia already has narrower reporting hooks that it could extend along these lines, though Texas pairs the mandate with services and staffing that carry real cost.

Pennsylvania: $30 million in state general fund cybersecurity investment (2024–2027, multisector)

- Governor Josh Shapiro invested $10 million per year in cybersecurity infrastructure from state general funds across 3 consecutive budget cycles, totaling $30 million over 3 years; this is not SLCGP money.

- The state frames the investment as protecting “critical data and services Pennsylvanians rely on.”
- While not labeled OT-specific, the investment signals that the state is willing to put its own dollars, not just federal pass-through funds, into cybersecurity at scale.
- It is relevant as precedent for any Virginia state-funded mechanism that sits alongside the federal program.

Key Takeaways for Virginia

Pennsylvania is a state that is committing its own general funds to cybersecurity at scale, separate from federal pass-through money, which is the precedent for any Virginia mechanism to reach private operators that federal grants cannot fund. The trade-off is that general fund commitments compete directly with other budget priorities, so this is the heaviest lift of the 6.

National context (Government Accountability Office, April 2025)

- As of August 1, 2024: The Department of Homeland Security had disbursed $172 million in SLCGP grants to 33 states and territories, funding 839 state and local cybersecurity projects aligned with NIST CSF functions.
- A federal bill (pending Senator John Cornyn’s reauthorization) would extend the SLCGP beyond fiscal year 2025 with a 60/40 funding split. Texas has received roughly $40 million over 3 years, among the highest state totals.
- Pennsylvania has added $10 million for cybersecurity in its 2026–27 budget from state general funds (separate from the federal grant program), bringing its total added cybersecurity investment to $30 million over 3 years.

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.



BlackJack3D via Getty Images

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.