MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

June 4, 2026

Dear Governor,

I write to you as the senior Senator for the Commonwealth of Virginia and its former Governor. I do so with urgency as the critical infrastructure in your state faces growing and underappreciated threats from adversaries wielding artificial intelligence (AI) tools capable of debilitating our national security, economy, and public health. This reality is worsened by the abdication of leadership at the Federal agencies charged with protecting America's critical infrastructure. As a result, your leadership in protecting critical infrastructure has never been more vital; I urge you to take the necessary steps to immediately harden that infrastructure to reduce vulnerabilities and defend your state and our nation. I encourage you to collaborate with your fellow governors, regionally and nationwide, along with the critical infrastructure and local leaders in your communities, to assess vulnerabilities, reevaluate risk tolerance for impacts caused by vulnerability remediation, and harden the critical infrastructure to intrusion and attack.

The dangers facing our critical infrastructure are real and, if realized, will be devastating. The interdependence of our critical infrastructure has inherent risk and creates cascading and cumulative harm. A successful attack on the power grid can disable water treatment operations. Disabled water treatment can shut down hospitals and schools. In even the most prepared and well-resourced region, this scenario would cause chaos and likely cost lives. Artificial intelligence has significantly lowered the barrier to entry for sophisticated, asymmetric attacks against critical infrastructure while simultaneously supercharging the capabilities of America's adversaries and criminal actors to disrupt our way of life. Ransomware attacks are increasing in both frequency and scale, AI-generated phishing is targeting the most vulnerable in our communities, and criminals and adversaries have automated AI to constantly scan critical infrastructure for vulnerabilities to exploit.

I have lived the challenge that you face in balancing competing priorities vying for your attention and resources, and it is with that knowledge that I urge you to place this issue at the forefront of your agenda. Not only because of the risk of not securing your critical infrastructure, but also because the federal backstop to support your state to defend its critical infrastructure has diminished. Since January 2025, the lead agency responsible for supporting states in critical infrastructure security and resilience, the Cybersecurity and Infrastructure Security Agency (CISA), has been without a full-time leader while losing approximately one-third of its workforce, including many senior leaders and cybersecurity and critical infrastructure subject

matter experts.[1] The White House terminated federal support for the Multi-State Information Sharing and Analysis Center (MS-ISAC), the decades-old program that provided free cybersecurity resources to 19,000 state, local, territorial, and Tribal members on the grounds that the MS-ISAC's work "no longer effectuate[d]"[2] the White House's priorities and banned federal grant recipients from using federal funds for costs associated with MS-ISAC membership.[3] The current proposed White House budget slashes CISA funding for a second year in a row, including reductions to CISA's budgets for cybersecurity, cyber operations, infrastructure assessments and security, security programs, security advisors, and intelligence.[4]

The gaps left by a weakened CISA and a defunded MS-ISAC are dangerous. I recognize that the unanticipated cost of MS-ISAC membership is out of reach for many and the fractured community defense hub makes your job harder. As you and your fellow Governors stand in the breach, there are concrete actions you can take today to better secure your critical infrastructure:

1. Convene a regional working group with state government and critical infrastructure owners and operators to establish a baseline for the tools, talent, and communication channels necessary to deploy the latest technology to not only identify and remediate vulnerabilities but anticipate and prevent future risks;
2. Direct a statewide critical infrastructure audit to identify the most vulnerable operators and fund mitigations;
3. Increase engagement with regional information sharing organizations, like fusion centers, that share threat intelligence and coordinate responses;
4. Identify under-resourced operators who lack baseline cybersecurity capacity and broker partnerships or funding mechanisms to bring them up to a defensible standard;
5. Demand the appropriate resourcing in funding and personnel for the federal agencies that partner with state and local governments, critical infrastructure owners and operators, and other stakeholders with the mission of preventing harm to U.S. critical infrastructure.

These are the risks that we all face – ask any critical infrastructure owner or operator and they will tell you that we are in bad shape, that they are worried, and they need CISA back to full strength, and soon. I am introducing legislation to restore CISA and the federal government's full capability to protect our critical infrastructure by reinstating and expanding federal funding for the MS-ISAC to ensure states, localities, Tribes, and territories can access the tools and information necessary to protect their critical infrastructure. The threats we face do not respect state borders or party lines and we cannot let those factors distract us from our task. Governors, and the federal government, are responsible for ensuring that critical infrastructure in their states,

---

[1]Doubleday, J. (2026, April 22). Plankey withdraws as CISA nominee. *Federal News Network*. https://federalnewsnetwork.com/cybersecurity/2026/04/plankey-withdraws-as-cisa-nominee/

[2] Wood, C. (2025, March 11). MS-ISAC loses federal support for threat intelligence, incident response. *StateScoop*. https://statescoop.com/ms-isac-loses-federal-support/

[3] Wood, C. (2025, August 4). New state, local cyber grant rules prohibit spending on MS-ISAC. *StateScoop*. https://statescoop.com/state-local-cyber-grant-msisac-2025/

[4] U.S. Department of Homeland Security, Office of the Chief Financial Officer. (2026, April 3). *CISA budget* [Budget document]. https://www.dhs.gov/sites/default/files/2026-04/26_0403_ocfo-budget-cisa.pdf

territories, and Tribal land are ready and resilient. The cost of inaction will be measured in disrupted services, damaged economies, and potentially lives lost — and that cost falls first on you and the people who trust you to keep them safe.

I invite you to coordinate with me directly to better protect your community – I will work alongside anyone committed to ensuring that when our adversaries test our critical infrastructure, it holds fast. Because the question is not whether our critical infrastructure will be targeted, but whether we will be ready when it is.

Sincerely,

Mark R. Warner
United States Senator