Ms. Kristin Darby
Chief Information Officer
State of Tennessee

Strategic
Technology Solutions

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

Hearing on:
"State and Local Cybersecurity: Evolving Threats, Federal Partnerships, and the Future of the State and Local Cybersecurity Grant Program"

May 21, 2026

Chairman Ogles, Ranking Member Ramirez, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today on behalf of the State of Tennessee.

I serve as the Chief Information Officer for the State of Tennessee and oversee Strategic Technology Solutions, the state's centralized information technology organization. Strategic Technology Solutions supports 21 executive branch agencies and approximately 45,000 state employees through enterprise technology, cybersecurity, infrastructure, and shared services. I also serve as Co-Chair of Tennessee's Artificial Intelligence Council and Co-Chair of the State Cybersecurity Council, helping guide statewide strategy related to cybersecurity resilience, artificial intelligence adoption, emerging technologies, and operational risk. In addition to supporting state agencies, Tennessee has adopted a whole-of-state approach to cybersecurity that emphasizes partnership, collaboration, and shared services with local governments across our 95 counties.

Cybersecurity is no longer a purely technical issue. It is a matter of public safety, economic security, and national defense. State and local governments operate the systems that citizens rely on every day, including emergency services, schools, utilities, and courts. These systems are now frequent targets of increasingly sophisticated cyber adversaries.

In Tennessee, we have taken a proactive, statewide approach to strengthening cybersecurity resilience. Through strong partnerships with federal agencies, local governments, and community organizations, we have made measurable progress. However, the pace and scale of cyber threats continue to outstrip the resources available at the state and local level.

State and local governments are being targeted at an unprecedented rate by both criminal organizations and nation-state actors.

We are seeing:

- Rapid growth in AI-enabled cyber attacks, accelerating both the scale and speed of adversary operations
- Increased reliance on supply chain compromise, including the integration of AI into widely used software tools
- Expansion of ransomware ecosystems and initial access brokers
- Greater exploitation of identity systems, cloud environments, and zero-day vulnerabilities

The reality is that adversaries no longer need weeks or months to exploit vulnerabilities. They can now move laterally across systems in minutes or seconds. At the same time, many local governments:

- Have little to no dedicated cybersecurity staff
- Operate with constrained budgets
- Depend on shared services or managed providers

In Tennessee, we have worked with local governments that were relying on part-time personnel or shared resources to manage critical systems supporting emergency services and public infrastructure. This creates an asymmetric environment where highly sophisticated attackers target the least-resourced defenders.

The rapid evolution of advanced large language models introduces a new category of cybersecurity risk that state and local governments are not yet fully equipped to manage. Emerging capabilities first observed in models like Mythos are accelerating the discovery and exploitation of vulnerabilities at a pace that challenges traditional defensive models. While government entities may have the opportunity to receive limited preview access to these technologies, the window between controlled release and broad availability continues to shrink, leaving little time for vendors to develop and distribute patches. Historically, vulnerability remediation has followed scheduled patching cycles, often monthly, but this paradigm is no longer sufficient. We are entering an environment that demands near real-time response, where mitigation may increasingly fall to government cybersecurity teams rather than product vendors due to this compressed vulnerability gap. This shift requires not only new operational models, but also flexible funding mechanisms that allow states to rapidly adapt. The State and Local Cybersecurity Grant Program (SLCGP) must remain nimble and capable of supporting these pivots to enable

investments in tools, processes, and workforce that can respond to an increasingly dynamic and AI-driven threat landscape.

Tennessee has adopted a whole-of-state cybersecurity model that emphasizes coordination, shared services, and partnership across state and local government. While we are not statutorily required to support local governments, we have chosen to do so because risk in one jurisdiction creates risk for the entire state.

Our statewide engagement has resulted in:

- Engagement of 1,500+ organizations across Tennessee
- Reached 3,000+ points of contact across public sector entities
- Achieved the #1 ranking nationwide in Nationwide Cybersecurity Review (NCSR) completions for both 2024 and 2025

Through this effort, more than 680 organizations became eligible for cybersecurity grant funding and nearly 300 organizations onboarded to MS-ISAC, gaining access to federal cybersecurity services. For organizations that participated consistently over three years, we observed a 19.2% increase in overall cybersecurity maturity.

This improvement is not theoretical, it reflects real advancements in:

- Threat detection
- Incident response
- Recovery capabilities
- Cyber governance

We have also seen strong gains across key sectors. School districts improved by more than 30 percent, public works entities improved by more than 28 percent, and cities and counties demonstrated steady, measurable progress. This demonstrates that when local governments are given the tools, guidance, and support they need, they can significantly improve their cybersecurity posture. Our focus has been on light touch, high impact solutions to enable this impact.

The SLCGP has been foundational to Tennessee's success. The State of Tennessee directed nearly all grant funding to local governments and retained only the minimal 5% for management and administration. All available funds have been fully allocated. This approach ensured that resources directly supported those with the greatest need.

While the approximately $28 million Tennessee received across four grant cycles has been impactful, the demand for cybersecurity support at the local level far exceeds current funding levels. Based on participation and identified needs through our statewide assessments, we could have effectively utilized several times that amount to expand protections, accelerate remediation efforts, and reach additional vulnerable entities.

To date, this program has enabled significant progress across Tennessee, including:

- Secured 89,684 endpoints across local governments
- Provided cybersecurity training to 21,236 local government employees

Funding has supported:

- Managed Endpoint Detection and Response (EDR)
- Cybersecurity awareness training
- Critical infrastructure improvements such as firewalls and disaster recovery systems
- Managed services for jurisdictions without IT staff

Tennessee intentionally focused on scalable solutions that minimize operational burden on local governments while providing enterprise-level security capabilities. Enabling participation by even the smallest and most resource-constrained jurisdictions has been critical to the progress the state has achieved.

Many local governments in Tennessee do not have dedicated IT staff. Several local entities participating in our program entered the process without basic protections such as endpoint monitoring, formal incident response capabilities, or centralized visibility into their environments. Without the grant program, they would be unable to deploy or sustain these cybersecurity capabilities. While Tennessee does not rely on federal funding for state-level cybersecurity operations, local governments depend heavily on the SLCGP.

While Tennessee has chosen to direct nearly all grant funding to local governments, there is also a strong case for allowing states the flexibility to use a portion of these funds to enhance state-level cybersecurity capabilities. States serve as central coordination points for threat intelligence, incident response, and shared services. Strengthening state infrastructure directly benefits local entities. Providing flexibility in how funds are applied would allow states to more effectively support a unified, whole-of-state cybersecurity posture.

Without continued funding:

- Local governments will lose access to critical services like EDR, which require ongoing subscription funding
- Many will be unable to sustain managed services or cybersecurity personnel
- Investments in infrastructure such as firewalls and disaster recovery systems will stall

Most importantly, we risk losing the momentum, relationships, and trust that have been built through our whole-of-state approach. Cyber adversaries are not slowing down. If funding and support diminish, the gap between attackers and defenders will widen.

State and local governments are now on the front lines of national cybersecurity. We are defending critical infrastructure, protecting sensitive citizen data, and responding to increasingly sophisticated cyber threats. However, states increasingly find themselves carrying this responsibility without sustainable funding models or adequate qualified workforce capacity. Based on Tennessee's experience, I respectfully offer the following recommendations:

1. Continued appropriated funding for the State and Local Cybersecurity Grant Program is necessary to sustain the progress states and local governments have made.

2. Provide Predictable, Long-Term Funding

- Enable states and local governments to sustain and mature their cybersecurity programs
- Avoid disruption of critical services

3. Lower and Stabilize Cost-Share Requirements

- Reduce financial barriers for participation
- Ensure rural and resource-constrained communities can continue to engage

4. Simplify Program Administration While Maintaining Accountability

- Streamline application and reporting processes
- Maintain appropriate governance and oversight

5. Expand Federal Support Services

- Increase availability of CISA no-cost services
- Address potential gaps created by reductions in MS-ISAC services

6. Improve Real-Time Threat Intelligence Sharing

- Provide immediate notifications for emerging threats and zero-day vulnerabilities
- Enable faster response at the state and local level

7. Address Emerging Risks, Including AI

- Expand program scope to include AI-enabled systems and operational technology
- Provide guidance and resources to secure evolving technologies

8. Establish Rapid Response Cybersecurity Funding Mechanisms
The current grant structure is not designed to address rapidly emerging threats that require immediate action.

- Create a dedicated federal funding mechanism for ad hoc cybersecurity needs as emerging risks arise
- Enable expedited approval processes that operate on timelines of days rather than months
- Allow states to respond quickly to zero-day vulnerabilities, active threats, and urgent remediation needs

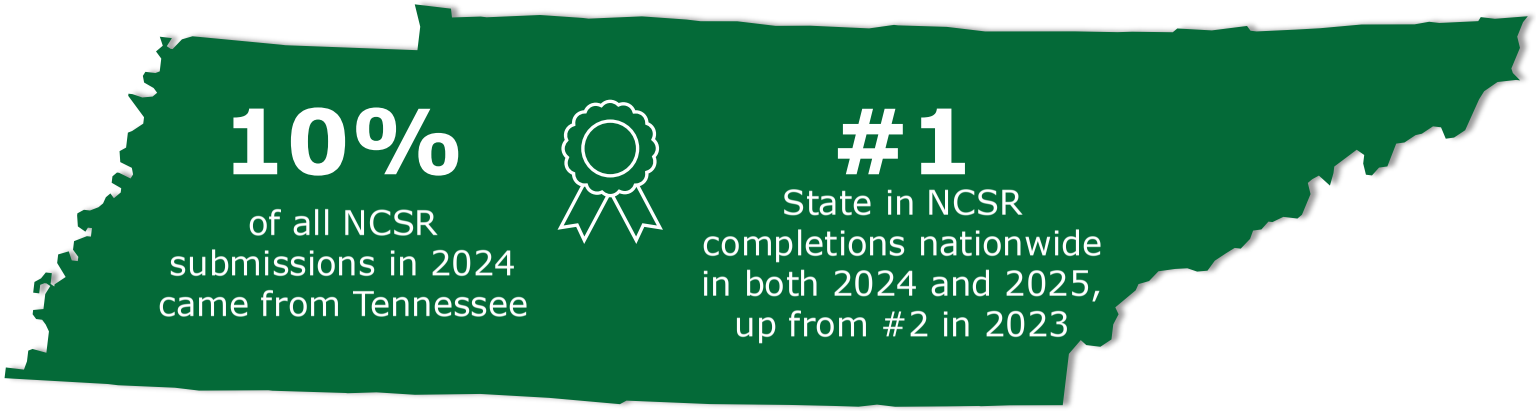
Tennessee has demonstrated that a coordinated, statewide approach to cybersecurity can produce measurable results. Through strong partnerships and targeted investments, we have improved cybersecurity maturity across a diverse range of local governments.

The scale, speed, and complexity of today's threat environment require sustained funding, operational flexibility, and the ability to respond at the pace of emerging threats. The State and Local Cybersecurity Grant Program is one of the most effective tools available to strengthen our collective defense. Reauthorizing and enhancing this program is essential not only for Tennessee, but for the security of the Nation.

Thank you for the opportunity to testify. I look forward to your questions.

Tennessee's Nationwide Cybersecurity Review (NCSR) Project

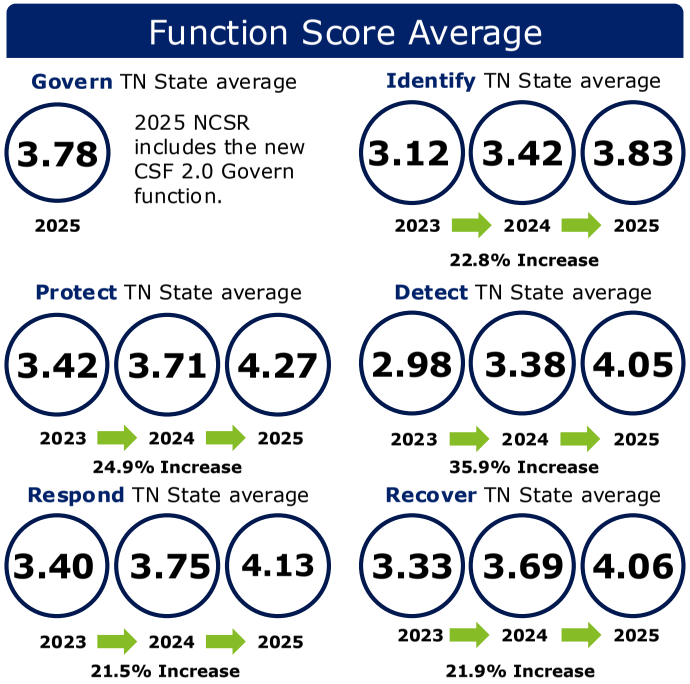
Since 2023, STS has led a statewide cybersecurity initiative — engaging 1,500+ organizations, reaching 3,000+ Points of Contact, and expanding access to assessments, grant funding eligibility, and cybersecurity support across Tennessee.



Tennessee NCSR Year to Year Maturity Improvement Journey

Strategic Technology Solutions

- Most recent 2023–2025 NCSR Completion Report provided by CIS
- Focuses on the 208 Tennessee organizations that completed the NCSR in all three years
- The NCSR uses a seven-point scale, where 7 is the highest possible score and 1 is the lowest



1. Not Performed | 2. Informally Performed | 3. Documented Policy | 4. Partially Documented Standards or Procedures | 5. Implementation in Process or Risk Formally Accepted | 6. Tested & Verified | 7. Optimized

**The percent change in this analysis reflects the change in average maturity score from the 2023 to 2025 NCSR cycles. The 2025 NCSR adopted the updated NIST CSF 2.0 question set, which may have caused scores for certain entity types to decrease in 2025 due to the addition of new questions to the assessment.*

Voices from TN Community Leaders

Strategic Technology Solutions

Organizations that have worked with the NCSR project team found the NCSR process approachable, informative, and helpful in identifying clear next steps.

"Completing the NCSR was beneficial in helping us think differently about the big picture of our IT infrastructure. Although we're a small town with no dedicated IT resources, ***completing the NCSR was attainable*** *and now we're eligible for grant funding to help us even more."*

—Middle TN Town Community Development Director

"Completing the NCSR and receiving our recommended Plan of Action & Milestones has been a ***great step in the right direction*** *for our cybersecurity plans. There is no ambiguity in what our next steps should be in becoming more cybersafe."*

—Middle TN County Leader

"Completing the NCSR has highlighted the NIST standard areas that our team has room to improve upon, ***making it clearer*** *how we can continuously improve our cybersecurity."*

— Tennessee State College Enterprise Application Leader

"I ***see the value in cybersecurity*** *even though my town is small. I've seen the effects of ransomware at a previous position."*

—TN Town Recorder

"The resources we have been given thus far have been ***really helpful****."*

—TN County School District Director of Technology

"Completing the NCSR has been an ***eye-opening experience*** *for me. I was unaware of the opportunities we have to improve our cybersecurity."*

—TN County School District IT Coordinator

Feedback from primarily rural organizations across Tennessee showed that the NCSR process successfully translated cybersecurity maturity into something **practical** and **actionable**.

"I love how ***you all broke that [Enhanced Recommendation] down****; it's so much easier to understand."*

—Middle TN City Recorder

"Really appreciate what you all are doing for the people of TN, this has been ***extremely informative****."*

—University Health Science Center Lead Cybersecurity Analyst

"The Plan of Action & Milestones was ***tremendously helpful*** *when tracking remediation activities."*

—TN City Systems Analyst

"I really like this PDF [Enhanced Recommendation]; it ***really helps with understanding****, and I can delegate assignments per tasks."*

—TN Town IT Manager

- Small cities/counties (population <50,000)
- Medium cities/counties (population 50,000 – 99,000)
- Other organization types