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 $21 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

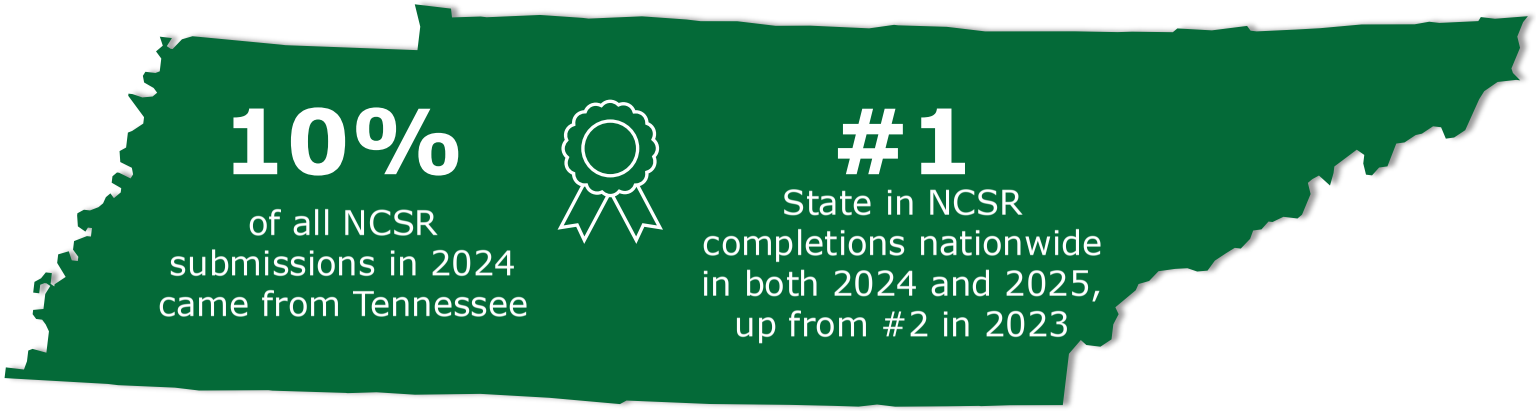
Tennessee has demonstrated that a coordinated, statewide approach to cybersecurity can produce measurable results. Through strong partnerships and targeted investments, we have improved cybersecurity maturity across a diverse range of local governments.

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.

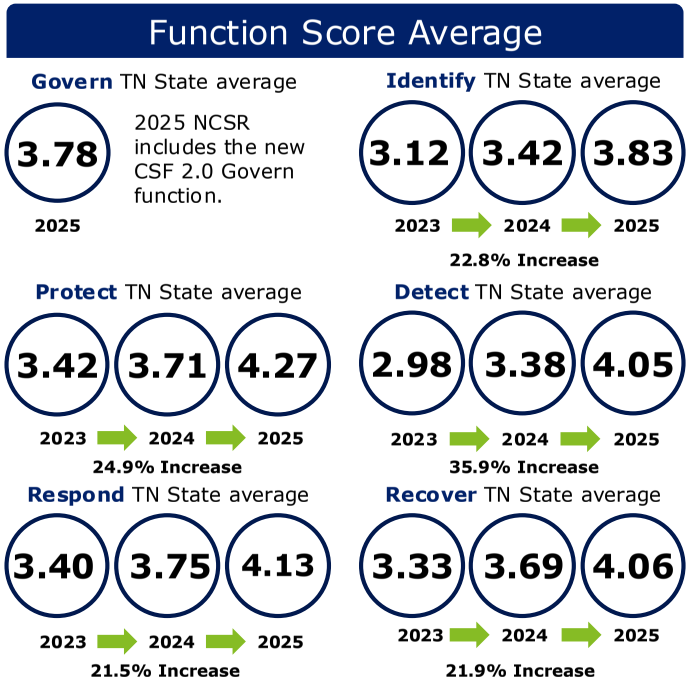
Tennessee's Nationwide Cybersecurity Review (NCSR) Project

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

- 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

"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**.

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

—TN County School District Director of Technology

"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

Tab 1

Executive Chamber

KATHY HOCHUL
Governor

COLIN AHERN
Director of Security and Intelligence

State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities

U.S. House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Testimony of:
Mr. Colin Ahern
Director of Security and Intelligence
New York State

Washington, DC
May 21, 2026

INTRODUCTION

Chairman Ogles, Ranking Member Ramirez, Chairman Garbarino, Ranking Member Thompson, and distinguished Members of the Subcommittee:

Thank you for the opportunity to submit testimony on the state of cybersecurity at the state and local level, the escalating threats facing America's communities, and the federal partnership needed to defend them.

Given the escalating threats we face today, this hearing could not be more urgent. Our states are on the front lines of multiple cyber conflicts, yet we are being asked to manage nation-state risks while our federal partners step back. It is a strategic failure that our primary federal partners and resources are being sidelined as threats escalate. From the imminent expiration of the State and Local Cybersecurity Grant Program (SLCGP), the shrinking of the Cybersecurity and Infrastructure Security Agency (CISA) and the lack of a Senate-confirmed CISA Director, to the cancellation of funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC), tools designed to keep our communities safe are being dismantled.

A functional partnership between federal, state and local governments, and the private sector is essential to reverse this trend. This partnership must be built on three key pillars. First, we need a Federal Government capable of detecting, mitigating, and responding to cyberattacks and deterring and punishing attackers across the operational spectrum. Second, we require robust collaboration with state and local governments and the private sector that facilitate rapid information exchange and operational coordination. Third, we need a private sector capable of defending its own systems and preventing attacks from originating within its infrastructure.

Currently, these pillars are being systematically undermined. Over the past year, the Trump administration has reduced funding for key offices and decommissioned collaboration mechanisms critical to our collective defense. By failing to address the risks of frontier AI, the administration has allowed the gap between the capability of nation-states and the capability of terrorist and criminal actors to vanish. This leaves under-resourced state and local governments, school districts, water utilities, and others

to face sophisticated adversaries alone. Without federal coordination for vulnerability disclosures, replacing legacy systems, and improved cyber defensive methodologies, we risk substantial, irreparable harm to our economy and our democratic way of life.

The State and Local Cybersecurity Grant Program has been a critical resource for state and local governments to defend our communities and continue to provide the services that the private sector and our people rely on. This program should be reauthorized and funded for the long term to provide sustained, stable resources to state and local governments facing growing threats.

My testimony outlines the threat landscape from the perspective of one of the largest states in the country and offers insights on our unique whole-of-state response and the results it has produced. I also lay out six recommendations for this Subcommittee and your colleagues in Congress to improve the resilience of America's communities by building better federal and state government partnerships.

I. THE THREAT LANDSCAPE

The cyber threat environment in 2026 is primarily being reshaped by two parallel forces. The first is a sustained, multi-vector campaign against U.S. critical infrastructure by nation-state, nation-state affiliated and supported adversaries, and transnational cybercriminals. The second is a rapid expansion of offensive capability driven by the maturation of frontier artificial intelligence (AI) and powerful open-weight models, in addition to the continued proliferation of highly professionalized cyber offensive capabilities to criminals and terrorists. Each of these forces is dangerous on its own. Together, they constitute the most consequential shift in the cyber threat picture since the emergence of nation-state cyber operations thirty years ago and the explosion of professional cybercriminal organizations with the advent of cryptocurrency fifteen years ago.

States are at the front lines of cyberattacks. New York’s history as a target of America’s adversaries is long and varied, stretching from the physical attacks on the World Trade Center; the cyber campaigns against our financial industry; and the scams targeting our

residents. Today, these physical and cyber threats have metastasized into a converged cyber-physical assault on our essential infrastructure. The public authorities, state and local governments, and municipal utilities that provide essential services like transportation, power, and clean water are being targeted by adversaries who do not respect state lines or national borders. We would never expect a local portmaster to repel a foreign warship steaming into a harbor, yet we leave the operational fabric of our communities to fend for themselves against the world's most sophisticated digital adversaries.

A. The Artificial Intelligence Inflection

Technical barriers that once limited sophisticated offensive cyber capabilities to an elite few are breaking down. Frontier AI and open-weight models, in their current generation, are already providing operational gains for our adversaries: the time from vulnerability discovery to working exploits has collapsed from weeks to hours;[1] thanks to deepfakes and other AI-enabled techniques, phishing emails can be nearly impossible to detect and are turbocharging ransomware attacks;[2] and sophisticated cyberattacks overall are rapidly increasing in frequency.[3] Without meaningful safety constraints on these models, including those controlled by competitors such as China,[4] the time, effort, and skill required for sophisticated cyber operations will exponentially decrease over the next six months, effectively democratizing sophisticated offensive cyber capabilities. The capability distinction between highly resourced and capable nation-state adversaries and everyone else – individuals, small groups, terrorist organizations, professionalized cybercriminals, and other non-nation state actors – is bound to collapse; the threat posed by actors capable of increasingly damaging and frequent cyberattacks will grow exponentially.

Traditional deterrence, which is already severely lacking, will fail completely in this modern threat environment. Non-state threat actors may be equipped with nation-state level capabilities with AI, but they are not bound by the same geopolitical or legal

[1] https://www.ibm.com/think/insights/the-mythos-moment-when-discovery-outpaces-defense
[2] https://go.crowdstrike.com/2026-global-threat-report.html
[3] https://mitsloan.mit.edu/ideas-made-to-matter/ai-cyberattacks-three-pillars-defense
[4] https://www.nist.gov/news-events/news/2026/05/caisi-evaluation-deepseek-v4-pro

pressures that deter nation-state adversaries from carrying out truly devastating cyberattacks on critical infrastructure. Because these non-state actors often operate outside this reach of conventional statecraft, we must focus even more forcefully on hardening our defenses to ensure attacks cannot succeed, and that we can rapidly recover from those that do.

To meet this challenge, we must mature our technology systems. At the state and local level, entities are plagued by legacy infrastructure and outdated technologies. Under-resourced critical infrastructure providers, school districts, and electrical and water utilities are already under severe strain from traditional adversaries, especially ransomware and were never designed to withstand a landscape of highly capable, AI-powered threat actors. This is why sustained federal resources through the PILLAR Act and the State and Local Cybersecurity Grant Program are essential, providing the funding needed to modernize fragile systems and deploy enterprise-grade defenses across our state and local governments. The time to act is now.

B. Nation-State Threats

Nation state threats have continued to advance against the United States and New York specifically. While their operational priorities differ, the strategic pattern is consistent: Nation state cyber threats are no longer limited to traditional espionage. They have expanded into three categories: prepositioning for destructive cyberattacks in critical infrastructure;[5] the theft of intellectual property and economic assets;[6] and the use of cyber capabilities to extend transnational coercion into our communities and generate revenue.[7]

Four nation-state actors drive the bulk of this activity: the People's Republic of China (PRC), the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea (DPRK). PRC operations have been publicly identified across U.S. telecommunications, water and wastewater, and energy sector systems, with March 2025 federal indictments confirming that Beijing operates a contractor

[5] https://www.congress.gov/crs-product/IF12798
[6] https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says
[7] https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforce ment-officers-global

ecosystem that serves as both an intelligence platform and a transnational repression apparatus. Russia continues to function as the principal sanctuary jurisdiction for the criminal ransomware ecosystem.[8] Iranian cyber activity continues to target energy, transportation, water, and government services.[9] DPRK cyber operations combine cryptocurrency theft and fraud, such as remote worker scams.[10]

Across all three categories, the convergence between criminal and state-aligned cyber activity described elsewhere in this testimony is no longer occasional. It is systemic. The same infrastructure, the same intermediaries, and increasingly the same techniques serve nation-state actors and the criminal ecosystems that operate adjacent to them. The defensive posture required to address active prepositioning, sustained theft, and adaptive coercion campaigns must operate continuously, with sustained federal partnership, sustained intelligence sharing, and sustained investment in the state and local capacity that defends the infrastructure and communities the Federal Government cannot reach directly.

C. Criminal Threats

The criminal threat surface is broad, lucrative, and accelerating. Phishing is the top cyber incident category reported to the State, and the days of ill-crafted phishing emails are long over. Cybercriminal groups now produce highly credible, often personalized lures that enable downstream fraud, data theft, and ransomware deployment.

The financial harm to New Yorkers is substantial. In 2025, the FBI's Internet Crime Complaint Center (IC3) ranked New York as the fourth among states in the following metrics: total reported complaint volume (45,255 complaints) and total victim losses (over $1.2 billion); cryptocurrency-related complaints (8,088 complaints) and related losses (nearly $600 million); and elder fraud losses (over $408 million).[11] The single

[8] https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-net work-controlled
[9] https://www.justice.gov/opa/pr/justice-department-disrupts-iranian-cyber-enabled-psychological-operations
[10] https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-techology-worker-0
[11] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

largest driver of those losses is investment fraud, dominated by the relationship-based cryptocurrency scams commonly called "pig butchering." The FBI attributes these schemes specifically to organized criminal enterprises operating from Southeast Asia, using trafficked workers as forced labor.

The theme again is one of convergence. The same criminal infrastructure that enables pig butchering also enables state-sponsored IT worker schemes, ransomware operations, and nation-state actors who obtain capabilities from professional criminal markets. Cryptocurrency mixers launder ransomware and investment-fraud proceeds. Cloud hosting providers enable both criminal and nation-state operators. Identity-laundering services supply both cybercriminal fraud rings and nation-state cyber operations. New York's 2023 Cybersecurity Strategy described this as the “convergence of criminal and nation-state actors.”[12] Three years on, that convergence is sharper, faster, and more difficult to disrupt. Treating cybercriminals and nation-state cyber threats as separate problems is a mistake, as they sit on top of the same plumbing, and federal action against both requires dismantling the infrastructure that serves them all.

II. NEW YORK’S WHOLE-OF-STATE RESPONSE

Governor Hochul's establishment of the Director of Security and Intelligence role in February 2026[13] built on several years of sustained investment in the State's cyber and hybrid threat capabilities, organized around the framework set out in the 2023 New York Cybersecurity Strategy and its principles of unification, resilience, and preparedness. The State's current operational posture rests on five mutually reinforcing components, each outlined in this section. Taken together, they constitute a model that other states are beginning to follow and that this Subcommittee should consider as a template for federal-state cyber partnership.

A. Unified Governance

The State has consolidated cyber, intelligence, and foreign-influence functions under unified senior leadership. This centralized structure allows the State to act coherently

[12] https://www.governor.ny.gov/sites/default/files/2023-08/2023-NewYork-CybersecurityStrategy.pdf
[13] https://www.governor.ny.gov/news/governor-hochul-appoints-new-york-states-first-ever-director-security-and-intelligence

when threats cross domains. It has also enabled the development of policies and programs which provide cybersecurity shared services to county and local governments, and privately owned critical infrastructure where appropriate and authorized by law.

B. Statewide Shared Services

The most operationally consequential State investment is the shared services model. As of May 2026, the State has deployed Endpoint Detection and Response (EDR) coverage on 102,806 endpoints and Attack Surface Management (ASM) across 105,725 assets in county and local government systems across New York. Additionally, utilizing State and Local Cybersecurity Grant Program (SLCGP) funding, the State is distributing more than 112,000 Multi-Factor Authentication (MFA) hard tokens to more than 160 eligible local government entities, school districts, and public authorities to secure identity access management. The savings to county and local governments over a three-year period is over $19 million – money that small jurisdictions, which would otherwise have no realistic path to enterprise-grade cyber tooling, can instead direct to essential services. Beyond the financial savings, the benefit of bringing these entities under the state’s umbrella to improve our whole-of-state cyber posture is invaluable.

The model produces results at every level of the defensive stack. In a single 30-day window in 2025, the EDR shared service identified and remediated 1,178 incidents across New York government entities, 509 of them categorized as high severity, 9 as critical, and 40 requiring human intervention. Over the same period, the State's proactive threat-hunting layer, which operates continuously around the clock, surfaced 28 distinct detections, of which 24 required further investigation. More than a dozen were adversary-in-the-middle attacks on state and local users, sophisticated session-hijacking operations of the type that, three years ago, were almost exclusively the province of well-resourced criminal groups and nation-state adversaries.

The most consequential measure of the program's effect is the one local government leaders care about most. Ransomware incidents reported to the State have declined from 14 in 2023, the year the shared-services investment began, to zero through the

first four months of 2026. This drop, despite increased reporting volume, is the strongest available evidence that investment in shared, state-level cyber defense generates significant returns.

Two operational examples illustrate the difference the shared-services model makes when an intrusion is actually underway. In 2024, the managed EDR service identified a malicious payload associated with a command-and-control framework on a county host following a user's interaction with a fraudulent government form. Detection, containment, and confirmed remediation took 37 minutes. A comparable hands-on-keyboard intrusion in the same period at a county without the managed EDR service took approximately 2,880 minutes, or two full days, to remediate. That difference can be what separates an incident from a crisis.

C. The Joint Security Operations Center and State Cyber Response Teams

New York operates one of the most robust state-level cybersecurity operations centers in the country. The Joint Security Operations Center, operated by the Office of Information Technology Services (ITS), supports State and local government missions 24/7/365. It ingests over 400 terabytes of data per month and processes approximately 350,000 security events per second. In 2025, the Joint Security Operations Center conducted more than 16,000 investigations leveraging over 24,000 detected events; expanded detection capabilities by 92 percent across 41 active use cases; and grew its staff by 33 percent to 65 analysts. The same year, ITS established a new partnership with the New York State Division of Military and Naval Affairs where State active-duty national guardsmen support the Joint Security Operations Center operations full-time in State Active Duty status.

D. Mandatory Cybersecurity Incident Reporting

New York requires municipal corporations and public authorities to report cybersecurity incidents to the Division of Homeland Security and Emergency Services within 72 hours, and to report any ransomware payments within 24 hours.[14] As of May 8, 2026, the State has received 202 mandatory reports. The reporting framework gives the State,

[14] https://www.governor.ny.gov/news/governor-hochul-announces-legislation-now-effect-strengthen-cyberscurity-across-new-york

for the first time, a real-time picture of the threats facing local government, and gives local governments a single coordinated channel for assistance. The reporting framework also enables critical cross-system defense: when a local government reports an account compromise or ransomware indicator, the State can identify accounts used by the affected entity, take precautionary action to reduce spillover risk to State systems, ensure timely and anonymized distribution of indicators of compromises to stakeholders, and ensure that an appropriate law enforcement response is undertaken.

Across State systems, ITS responded to 132 cyber incidents in 2025, a 45 percent increase since 2024. Across local government systems, the Cyber Incident Response Team (CIRT) within the Division of Homeland Security and Emergency Services responded to 145 incidents in 2025 and 157 incidents in the 2026 calendar year through May 8, 2026. The growth in CIRT reporting volume reflects both an expanding threat surface and improving reporting fidelity from a mandatory reporting framework that did not exist eighteen months ago. New York State has continued to grow its law enforcement capabilities as well, including an additional $7.4 million to expand the New York State Police's Cyber Analysis Unit, Computer Crimes Unit and Internet Crimes Against Children Center.[15]

E. Frontier Technology

New York has moved aggressively to address emerging technology threats that federal action has not yet caught up to. In June 2025, Governor Hochul signed the Responsible AI Safety and Education (RAISE) Act, one of the country's first state-level safety frameworks for frontier AI developers.[16] The RAISE Act requires large developers to conduct cyber capability evaluations of frontier models prior to deployment. It requires those developers to report when they detect their models being used in cyber operations against critical infrastructure. And it requires reporting when a developer's model materially contributes to a catastrophic-risk event, defined in statute as a single incident causing more than fifty deaths or serious injuries or more than one billion dollars in damages, where the model provided expert-level assistance in creating a

[15] https://www.governor.ny.gov/news/governor-hochul-announces-nation-leading-cybersecurity-strategy
[16] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20251222

weapon of mass destruction, engaged in unsupervised cyberattack or serious criminal conduct, or evaded developer or user control.

III. RECOMMENDATIONS TO THE SUBCOMMITTEE

The State's experience yields six specific recommendations for consideration by this subcommittee and your colleagues in Congress.

1. Reauthorize and Fully Fund the State and Local Government Cybersecurity Grant Program via the PILLAR Act

The State and Local Cybersecurity Grant Program (SLCGP) is the single most consequential federal investment in the cyber protection of municipal services, public utilities, school districts, and State and local governments in this country. Without reauthorization via the PILLAR Act, the consequences for state and local cyber defense will be immediate and severe. Programs that states have built up over three years cannot be sustained at current scale without more financial support. And in a meaningful number of cases, programs initiated with SLCGP funding will simply shut down, taking the cybersecurity posture of the jurisdictions they serve with them. The PILLAR Act should be the floor, and the program should be robustly funded for the long term.

Four operational adjustments would meaningfully improve the program at reauthorization:

1. The cost-share match requirement is difficult for cash-strapped state and local jurisdictions, and disproportionately burdens the smaller jurisdictions for which the program is most critical. Elimination or substantial reduction of the match should be considered.
2. Funding should be reauthorized at a consistent multi-year level so that states can plan multi-year procurements, vendor relationships, and shared-services contracts against a stable horizon. State input on program priorities prior to release of funding would also improve operational fit, especially to make it easier to engage in software-as-a-service, multi-year, statewide shared services.

3. The current rural/urban percentage allocation structure should be removed or adjusted as it makes it difficult for states to procure sophisticated shared services that benefit all jurisdictions. Removal of these percentage requirements, or a substantial mitigation of them for shared services available for all, would allow states to deploy modern enterprise-grade tooling across mixed-jurisdiction portfolios.
4. Current restrictions that prevent SLCGP funds from being used to purchase Multi-State Information Sharing and Analysis Center (MS-ISAC) memberships and services should be removed. This restriction is contrary to the program's stated purpose. The MS-ISAC, operated by the nonprofit Center for Internet Security, provides nationally sourced threat intelligence, incident response support, and competitively priced cybersecurity tooling to public sector entities at a scale no individual state can replicate cost-effectively. A statewide MS-ISAC membership is among the highest-leverage uses of SLCGP dollars available, particularly for more than 20,000 SLCGP-eligible entities in New York alone, the majority of which are small, rural, or under-resourced jurisdictions.

2. End the Two-Tiered Defense in Artificial Intelligence Access

Frontier AI is collapsing the time between vulnerability discovery and exploitation. State and local governments protect the power grid, the drinking water supply, public health systems, school districts, insurance, and the everyday operations of government. These systems provide more direct services to more Americans than the federal systems for which advanced defensive AI tooling is currently being scoped. Yet state and local cyber defenders have limited structured pathways to the same class of frontier AI capabilities that federal partners and a small number of large enterprises are beginning to access.

The need to address this access gap extends across all levels of government and across both parties. On May 13, 2026 a bipartisan group of thirty-two House members wrote to the National Cyber Director calling for, among other things, "expanded controlled defensive access" to frontier AI for trusted defenders and a framework for managing AI discovered vulnerabilities at scale.[17] This follows a May 4, 2026 joint letter

[17] https://latta.house.gov/uploadedfiles/ai-discovered_vulnerability_coordination_letter.pdf

from 14 states, led by New York,[18] which called for AI companies to better consider and include state, local, and critical infrastructure equities in the development and deployment of their models.

New York is already working with private-sector partners to incorporate frontier AI into its defensive posture. We must establish a structured program through which state fusion centers and state operations centers including New York's JSOC receive priority access to current and future frontier defensive AI capabilities at the same time those capabilities are made available to federal partners and large technology companies.

3. Restore the Federal Government's Capacity to Be a Partner

CISA has lost approximately one-third of its workforce in the past year.[19] The operational consequence in New York is that CISA's availability to State agencies and local governments has materially diminished. The quantity and quality of cyber threat intelligence delivered to states by CISA and the Department's Office of Intelligence and Analysis has declined, including the frequency of classified briefings for cleared personnel.

Congress should resource the CISA workforce to the level the mission now requires.

Six specific items merit congressional attention.

1. CISA should be resourced and authorized to conduct its mission. The cuts to the CISA workforce should be reversed, and CISA should leverage state and regional Fusion Centers as a force multiplier. Fusion Centers maintain the local contacts and trust relationships that allow federal threat reporting to be operationalized at speed. Providing training and dedicated resourcing to Fusion Centers with a cyber component would give CISA proactive reach into communities it currently cannot serve directly.
2. CISA needs consistent, Senate-confirmed leadership to navigate long-term strategic threats and to serve as a stable partner to the states. Acting and vacant

[18] https://www.governor.ny.gov/sites/default/files/2026-05/Joint_Letter_State_Access_Frontier_Models_4MAY2026__.pdf
[19] https://federalnewsnetwork.com/cybersecurity/2026/04/cisa-cyber-partnerships-face-standstill-amid-cuts/

senior roles cannot drive the multi-year coordination required to meet adversaries who operate on a long planning horizon.

3. The Cybersecurity Information Sharing Act of 2015 expires on September 30, 2026. The Act is the legal foundation for the voluntary information sharing among the private sector, the Federal Government, and the states that defend critical infrastructure. Another short lapse will further chill the private-sector reporting that CISA and state cyber operations centers rely on.
4. The Nationwide Cybersecurity Review (NCSR) program has been discontinued. NCSR was a free, annual, anonymous self-assessment tool that local governments used to benchmark cybersecurity maturity against peers, identify gaps, and meet federal grant eligibility requirements, including for SLCGP itself. Its loss creates immediate friction in grant compliance and removes a critical maturity-measurement tool from the field. Restoration of NCSR, or a functional federal equivalent, should be a near-term priority.
5. CISA should complete rulemaking for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and finalize the national reporting framework for critical infrastructure cybersecurity incidents. New York, alongside a group of other states with elected leadership from both parties, provided formal comments on CIRCIA highlighting the importance of federal and state reporting requirements to be harmonized and actionable.[20] The final rule should also include a structured mechanism for CISA to notify state regulators when entities they oversee report covered incidents.
6. CISA should re-establish the Critical Infrastructure Partnership Advisory Council to restore the formal collaborative environment between state and local governments and the private sector. As part of this effort, CISA should designate cloud service providers and major data centers as critical infrastructure, as these environments are critical for state and local governments and critical infrastructure.

4. Establish a Federal Floor for Frontier AI Safety with Reporting Obligations

[20] https://www.regulations.gov/comment/CISA-2022-0010-0458

The Federal Government should establish a regulatory framework for frontier AI development that prevents the proliferation and misuse of cyber-offensive capabilities which threaten homeland security. The framework should be harmonized with the operational requirements of the New York RAISE Act and should include three elements at minimum: pre-deployment cyber-capability evaluations by large developers, with results shared with federal, state, and local stakeholders; mandatory reporting when developers detect their models being used in cyber operations against critical infrastructure; and mandatory reporting of catastrophic-risk events like those defined in the RAISE Act statute.

Federal action of this kind would give industry a single national floor for transparency and safety obligations, and give state and federal defenders the visibility they need to act on emerging risks. It should not, however, preempt state regulation that goes further. States carry the operational consequences of frontier AI deployment most directly, through our critical infrastructure protection, public safety, financial services, and consumer protection authorities. New York's RAISE Act was enacted because federal action has not developed at a pace equal to the evolution of risks. We cannot afford to lose what we have built while waiting for federal action that may or may not come, and that may or may not match the threat.

5. Modernize the Federal Legal Framework for Cyber Prosecutions

Defense and resilience are not sufficient on their own. The Federal Government also must impose consequences on cyber actors, including the transnational criminal organizations that account for the bulk of consequential criminal cyber activity against U.S. targets. Two changes would meaningfully expand that capability.

1. The Cyber Conspiracy Modernization Act,[21] introduced on a bipartisan basis should advance. The bill would allow conspiracy charges under the Computer Fraud and Abuse Act, with penalties scaled to the severity of the underlying conduct. The bill's conspiracy provisions should also be extended to reach those

[21] https://www.rounds.senate.gov/imo/media/doc/cyber_conspiracy_modernization_act.pdf

who knowingly provide or facilitate "bulletproof" hosting infrastructure for cyber crime that enables both criminal and nation-state operators.

2. Federal training programs like the Secret Service's National Computer Forensics Institute[22] provides training for prosecutors on digital evidence and cybercrime. Expanding federal capacity to train law enforcement to investigate these crimes would meaningfully accelerate prosecutor capacity nationwide.

6. Address Cyber Crime on U.S. Infrastructure

The current operating environment enables criminals to spin up cloud computing, purchase infrastructure, and launder cryptocurrency transactions in minutes. Each of these is the product of legitimate U.S. industry. Each is also a force multiplier for fraud, ransomware, account takeover, disinformation, foreign malign influence, and sanction evasion. Pig butchering operations, laptop farms that placed operatives inside dozens of New York-area companies, cyber espionage and attackers, and ransomware crews all rely on the same American-hosted infrastructure to scale.

Frictionless cyber crime on U.S. infrastructure is not an inevitability. It happens on infrastructure that American companies operate and that American law governs. Making that infrastructure harder to reach for our adversaries is one of the most consequential cyber actions Congress can take. Congressional action should focus on three areas.

1. The major cloud and hosting providers should be required to implement and document meaningful know-your-customer and abuse-response practices, with clear federal authority to act when those obligations are not met. The current model relies on voluntary self-regulation that has not kept pace with the threat. A graduated federal framework would create real consequences for providers who knowingly host criminal operations and clear safe harbors for those who do not.
2. Addressing the fraud facilitated by cryptocurrency exchanges requires decisive federal action. The current regulatory gap has allowed predatory scams like pig butchering, sanction evasion, ransomware, and other crimes to flourish at scale. To stop this predictable harm, the Federal Government should implement a

[22] https://www.secretservice.gov/investigations/cyber

national regulatory floor modeled on the New York Department of Financial Services' BitLicense Program, which enforces strict consumer protection, cybersecurity, and capital adequacy requirements.[23] This would help choke off illicit pipelines while maintaining a stable, predictable environment for legitimate crypto enterprises.

3. The Federal Government should accelerate its disruption authorities. The Department of Justice's disruptions of nation-state and cybercriminal groups' cyber operations show that targeted takedowns work when properly resourced.[24, 25, 26] Congress should ensure those authorities, and the cross-agency coordination they require, have the staffing, the funding, and the legal clarity to scale to the current threat environment.

IV. CONCLUSION

Cybersecurity is the silent partner of democracy. When the public utilities, school districts, state agencies, and county governments that constitute the operational fabric of American life are hollowed out by cyberattacks, the institutions that prop up democratic life are hollowed out with them. Reauthorizing the PILLAR Act, restoring federal coordination capacity, opening frontier defensive AI to state defenders, regulating frontier AI development at the federal level without preempting states, modernizing cyber prosecution authorities, and rejecting frictionless cyber crime as a policy default are not six separate items. They represent six elements of a single proposition: that the institutions of self-government in this country are worth defending against threats that do not respect state lines or national borders. Doing so demands the Federal Government to be a partner to all 50 states.

New York is ready to do its part. We want and need the Federal Government as our partner in the work.

---

[23] https://www.dfs.ny.gov/virtual_currency_businesses
[24] https://www.justice.gov/opa/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology-worker
[25] https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-dns-hijacking-network-controlled
[26] https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

Ron DeSantis, Florida Governor
Tom Berger, Interim Secretary
Warren Sponholtz, State Chief Information Officer

Testimony of Warren Sponholtz

State Chief Information Officer and Director, Florida Digital Service

State of Florida

Before the U.S. House Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities

May 21, 2026

Opening Statement

Chairman Ogles, Ranking Member Ramirez, and Members of the Subcommittee: thank you for the opportunity to appear before you today. My name is Warren Sponholtz, and I serve as the Chief Information Officer for the State of Florida and Director of the Florida Digital Service. I appreciate the Subcommittee's attention to the cybersecurity threats facing state, local, tribal, and territorial governments, and to the federal partnerships that help communities defend essential services.

Under Governor DeSantis' leadership, Florida approaches cybersecurity from a simple premise: cyber risk is not just an information technology issue. It is continuity of government, public safety, emergency response, critical infrastructure protection, economic stability, and public trust. The systems we defend support licensing, benefits, elections, law enforcement, education, health, water, transportation, and the many other services Floridians expect to be available every day.

Threat Landscape

The cyber threat picture facing Florida has two faces. The first is financial: criminal groups that steal data, disrupt operations, and demand payment. The second is geopolitical: foreign governments that seek access to the systems Americans rely on so they can steal information, position themselves for future disruption, or weaken confidence in public institutions. Florida sees both, we plan for both, and we do not treat either as theoretical.

Florida is a large and attractive target. We are the third-most populous state in the nation, with roughly 23 million residents. The state enterprise includes 35 state agencies, more than 107,000 employees, and approximately 202,000 devices. State law also gives Florida a role in supporting cybersecurity across nearly 500 counties and municipalities. Florida is home to major military commands, space assets, ports, airports, utilities, hospitals, schools, and public safety networks. An adversary does not look at those responsibilities as separate silos. An adversary sees one target. Our job is to build one coordinated defense.

The threat environment has changed substantially in recent years. Ransomware remains a persistent risk for counties, cities, school districts, Sheriff's offices, utilities, hospitals, and state agencies. These groups are not

always highly sophisticated in the way the public imagines. Often, they use stolen credentials, exploit unpatched internet-facing systems, or rely on social engineering. But their operating model has become highly organized. Ransomware is now an ecosystem: operators, affiliates, brokers, negotiators, data-leak sites, and money-laundering services. Taking down one brand does not end the threat; affiliates can migrate to another platform and continue targeting public services.

At the same time, nation-state activity has become more operationally significant for state and local government. China, Russia, Iran, and North Korea present distinct cyber risks to the United States. Of those, the activity associated with China has changed the conversation most directly for critical infrastructure. Campaigns commonly referred to as Volt Typhoon and Salt Typhoon demonstrate that foreign adversaries are not only seeking data. They are positioning themselves in communications, energy, water, transportation, and other critical sectors in ways that could matter during a future crisis. For Florida, that means our threat intelligence program must look not only for obvious disruption, but also for quiet, long-term access that may be designed to remain undetected for years.

Florida's Coordinated Defense Model

That is why Florida has moved toward a federated but highly orchestrated model of cyber defense. The goal is not to centralize every technology decision. The goal is to create coordination, visibility, speed, and trust across a very large and diverse public-sector environment. State agencies, local governments, educational institutions, law enforcement, emergency management, federal partners, and private-sector critical infrastructure providers each have responsibilities. The state can add value by creating common capabilities, sharing intelligence, coordinating response, and helping smaller entities reach a security baseline they could not afford alone.

Cybersecurity Operations Center

The center of that effort is Florida's Cybersecurity Operations Center, or CSOC, within the Florida Digital Service. The CSOC serves as the state's central threat clearinghouse. It monitors threats across the state enterprise, supports incident response, and helps agencies and partners move from isolated alerting to coordinated detection and response. The CSOC provides incident response assistance to agencies, local governments, and educational institutions. It deploys on-site resources to assist in recoveries and has supported election security in partnership with the Florida Department of Law Enforcement, the Florida Department of State, and the Florida Division of Emergency Management. Maintaining our CSOC has long been a priority for the Governor through his support of recruiting top-tier responders and funding technology enhancements for the important work it handles.

We are also moving the CSOC from a traditional alert-monitoring function toward a more proactive intelligence and analytics operation. That includes advanced analytics for threat hunting, anomaly discovery, behavioral analysis, and enterprise-wide correlation. The objective is straightforward: detect threats earlier, contain them faster, recover more effectively, and maintain government services.

Threat Intelligence and Federal Partnership

Threat intelligence is central to that mission. Florida's intelligence program draws from CISA, federal law enforcement, multistate partners, cybersecurity vendors, managed security providers, proactive threat hunts, incident response activity, and monitoring of criminal marketplaces. But intelligence is only useful when it is operationally relevant. A generic alert about a vulnerability is not enough. Agencies and local partners need timely, contextual information: what is being exploited, where it is likely to matter, what systems may be exposed, what action is expected, and how urgently it must be taken.

Shared telemetry is what makes that possible at scale. When participating entities share security telemetry with the state, Florida can correlate activity across environments. A threat identified in one county, agency, utility, or school system can become a defensive action for others. This is one of the most important benefits of a whole-of-

state approach. It turns separate organizations into a distributed sensor network and allows the state to deliver warnings that are specific, fast, and actionable.

The federal government is an essential partner in this work. Federal intelligence collection and sharing brings national visibility that no individual state can replicate. Federal advisories, threat feeds, automated indicator sharing, vulnerability guidance, and incident coordination help states understand what is happening across the country and what may be heading toward our jurisdictions. Florida adds state and local context to that national view. We understand our agencies, local governments, critical infrastructure operators, emergency management structures, and regional constraints. The best outcomes come when national intelligence and state-level context are combined quickly and operationally.

That partnership has become more important as the threat landscape has changed over the past three years. State and local governments are no longer dealing only with isolated ransomware events or opportunistic criminal activity. We are now defending against a faster, more industrialized criminal ecosystem; increased targeting of schools, utilities, hospitals, and public safety systems; and nation-state activity that is increasingly focused on critical infrastructure and operational disruption.

Enterprise Resilience and Governance

Florida's resilience strategy is broader than any single tool. It includes assessments to identify weaknesses, standards to establish consistent expectations, training to develop cyber skills, remediation support to close known gaps, incident response coordination, and communities of practice that bring security leaders together before an incident occurs. Those relationships matter. During a cyber incident, trust built in advance can reduce confusion, accelerate decision-making, and limit the impact on residents.

Florida has also taken action to reduce risk from applications tied to countries of concern. Governor DeSantis signed legislation enabling prohibited applications to be identified and removed or restricted from government-issued devices, with a defined waiver process for specific mission needs. That is a practical example of governance in action. It is not enough to wait for an incident. We must reduce exposure before applications, vendors, or platforms become operational risk.

Critical Infrastructure Protection

Critical infrastructure is a major focus of Governor DeSantis' strategy. Florida continues to work with critical infrastructure providers to better understand where investment is needed and where systemic risk exists. Through the diligent efforts of the University of South Florida, we have collected useful information from critical infrastructure assessments across the state. We also use the Department of Energy's Cybersecurity Capability Maturity Model to support more consistent discussions about risk, maturity, and priority investments. This is especially important in operational technology environments such as water and wastewater systems, utilities, transportation systems, public safety communications, and industrial control systems. These environments often cannot be secured in the same way as traditional office networks, and many smaller operators lack dedicated cybersecurity staff.

Florida Local Government Cybersecurity Grant Program

Florida's state-funded Local Government Cybersecurity Grant Program is one of our most important tools for reaching local communities. Rather than simply issuing direct payments, the Florida Digital Service procures cybersecurity capabilities on behalf of participating local governments. That model creates economies of scale, reduces procurement friction, gives smaller entities access to enterprise-grade solutions, and helps ensure that deployed tools contribute to a statewide defense architecture. Through Governor's DeSantis' leadership and in partnership with the Florida Legislature, the program has been funded at $30 million, $40 million, and $15 million over the past three funding cycles, respectively.

The capabilities provided through the state program include asset discovery, endpoint detection and response, email security, content delivery network protections, identity and access management, attack-surface management, extended detection and response, and related security operations capabilities. These are foundational controls. Many rural and fiscally constrained communities know they need these protections but cannot obtain them at the scale, speed, or price available through a state-coordinated procurement model. Emphasizing these rural and fiscally constrained communities has been a targeted focus area for Governor DeSantis and the Florida Digital Service.

This program also strengthens statewide visibility. In the current application cycle, Florida received 226 applications, and approximately 90 percent of applicants indicated they were willing to share telemetry with the State CSOC. That willingness is important. It reflects growing trust between the state and local partners, and it enables a more mature defense model in which local investments improve not only the applicant's security, but the security of the broader public-sector ecosystem.

Federal State and Local Cybersecurity Grant Program

The federal State and Local Cybersecurity Grant Program, or SLCGP, complements Florida's state-funded model. In Florida, the federal program is managed through the Florida Division of Emergency Management, with cybersecurity subject matter expertise from the Florida Digital Service. The current focus areas are law enforcement and critical infrastructure, where many needs fall outside the standardized technology bundles provided through the state program. Florida received 66 applications in the current cycle, including applications from 45 cities, 16 counties, and 5 other entities such as water management districts. Fourteen applications were law-enforcement specific.

SLCGP Project Examples

The projects submitted under the federal program illustrate why flexibility matters. One proposed water treatment project would make a high-service pump remote input/output system independent from its main controller, helping the process continue operating during a controller failure or cyber incident. Another project would modernize a city's water and wastewater telemetry system by replacing outdated radio units at a master control site and 35 remote lift stations with more secure and redundant communications. A rural Sheriff's office proposed securing mobile data terminals used by deputies to access dispatch, records, and license plate reader systems in the field. These are not abstract technology upgrades. They are investments in public health, public safety, and continuity of essential services.

The federal program also helps address continuous risk assessment across critical infrastructure and law enforcement environments. One proposed Florida project would provide recurring attack-surface and attack-path analysis for participating critical infrastructure entities and Sheriffs' departments. That type of visibility helps decision-makers understand where vulnerabilities exist, how they could be chained together by an attacker, and which remediation steps would reduce the most risk. For local entities with limited staff, that analytical support can be the difference between guessing and prioritizing.

Another proposed use of SLCGP funding would allow Florida to purchase an enterprise governance, risk, and compliance platform for state agencies. Today, cybersecurity risk information often lives in separate assessments, spreadsheets, plans of action, audit responses, and supporting artifacts. A shared platform would give the state a more consistent way to collect assessment results, score and prioritize cybersecurity risks, track remediation over time, and maintain a catalog of relevant evidence and artifacts. That capability would strengthen enterprise risk governance, improve accountability, support reporting requirements, and help state leaders make better investment decisions across agencies.

Long-Term Federal Partnership and Reauthorization

The SLCGP has helped make that partnership real. It has supported planning, assessments, implementation, and collaboration across the country. It has helped rural communities, small governments, schools, counties, and critical infrastructure operators work on basic cyber hygiene and more advanced resilience needs. It has also encouraged state and local officials to meet before an incident occurs. That may be one of the program's most valuable effects: it creates relationships, governance structures, and shared plans before a crisis.

For those reasons, long-term reauthorization matters. Florida is building long-range cybersecurity plans. The PILLAR Act is complementary to these plans and the direction Florida is already moving. It recognizes the need for sustained federal partnership, supports rural communities, strengthens critical infrastructure and operational technology protections, and accounts for emerging issues such as artificial intelligence and improved intelligence sharing.

At the same time, reauthorization should preserve practical access for the communities that need the program most. High or unstable match requirements can discourage participation, especially among rural and fiscally constrained entities. Reimbursement models can also be difficult for smaller communities that cannot carry large up-front costs. Federal grant design should make it easier for the most vulnerable communities to participate. Additionally, I would be remiss if I did not advise thoughtful caution with AI as it continues to scale into our lives and in these cybersecurity discussions. Disclosure of interactions with AI, protecting minors through parental notification/consent, and safeguarding personal identifying information and sensitive data are all principles we keep in mind in Florida.

Lessons for State and Local Cybersecurity

Florida's experience leads to several lessons. First, shared services work when they are paired with trust and clear governance. Second, telemetry sharing is essential for speed and correlation, but it must be built through partnership, not mandate alone. Third, critical infrastructure protection requires both IT and operational technology expertise. Fourth, smaller governments need procurement support as much as they need funding. Fifth, incident response is strongest when relationships and exercises happen before the emergency.

Cybersecurity as a Sustained Mission

I also want to emphasize that cybersecurity is a sustained operational discipline. It is not a one-time project. New vulnerabilities appear every day. Criminal groups reorganize. Nation-state actors adapt. Local governments replace equipment slowly. Workforce shortages persist. Artificial intelligence will create both defensive opportunities and new risks. The public sector needs funding models, shared services, and governance structures that recognize this as a long-term mission.

Florida has made meaningful progress under the leadership of Governor DeSantis: We have built a central cybersecurity operations capability, expanded incident response support, strengthened state and local collaboration, improved enterprise visibility, reduced costs through shared capabilities, and created grant models that help local governments obtain protections they could not easily acquire alone. But the threat landscape is moving quickly, and we must continue to move with it.

Conclusion

The adversary does not distinguish neatly between a state agency, a small city, a water utility, a school district, a Sheriff's office, or a critical infrastructure provider. To the adversary, those are all pathways into public services and public trust. Our defense must be equally connected. Continued federal partnership and information sharing, sustained support for the SLCGP, and long-term reauthorization through legislation such as the PILLAR Act will help states build that connected defense.

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

CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of Samir Jain
Vice-President of Policy, Center for Democracy & Technology

For the U.S. House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection
Hearing Entitled "State and Local Cybersecurity: Escalating Threats, Federal Partnership, and the Resilience of America's Communities"

Thursday, May 21, 2026

Chair Ogles, Ranking Member Ramirez, Chair Garbarino, Ranking Member Thompson, and distinguished Members of the Committee: thank you for the opportunity to testify today on the cybersecurity threats facing state and local governments and the critical role of the federal government in helping to meet them.

My name is Samir Jain, and I am the Vice President of Policy at the Center for Democracy & Technology (CDT), a nonpartisan, nonprofit organization that has worked for more than three decades to advance civil rights and civil liberties in the digital age. CDT brings deep expertise across cybersecurity, privacy, civic technology, elections, and artificial intelligence policy. We engage directly with federal agencies, state and local officials, the private sector, and civil society to promote a more secure and trustworthy digital ecosystem.

State and local governments today are confronting serious cybersecurity threats across nearly every domain in which they operate, from the critical infrastructure that powers our communities and schools, to the systems that administer our elections, to the public benefit programs that millions of Americans rely on for health care, food assistance, and basic income support. When these systems are compromised, people can lose access to critical resources and services at the moments they need them most. Their most sensitive personal information—Social Security numbers, medical records, financial data, immigration status, and information about their children—can be exposed to criminal actors and foreign adversaries, leading to identity theft, financial fraud, harassment, and other harms that can take years to recover from.

A pernicious knock-on effect of these incidents is the erosion of public trust. When Americans see their state DMV, their county hospital, or their child's school district suffer a major breach, their confidence that the government can serve them effectively and handle their personal information with care is shaken. That erosion of trust has consequences far beyond any single incident: it can deter people from enrolling in benefits to which they are entitled, from registering to vote, or from comfortably engaging with public institutions.

These risks are only heightened as artificial intelligence creates new opportunities for malicious actors to attack and exploit government systems at unprecedented speed and scale. The recent announcement of advanced AI systems with substantial cyber capabilities, such as the Mythos Preview from Anthropic, has made clear that the offensive cyber landscape is poised to change dramatically, and small and under-resourced jurisdictions are likely to be particularly vulnerable to that change.

Previously, the federal government has played an indispensable role in helping state, local, tribal, and territorial (SLTT) governments meet these challenges. Through dedicated grant programs such as the State and Local Cybersecurity Grant Program (SLCGP) and through technical assistance from the Cybersecurity and Infrastructure Security Agency (CISA), state and local officials have received targeted funding, threat intelligence, vulnerability assessments, network monitoring tools, tailored guidance, and incident response support. The federal government has offered unique capabilities that no individual state can match: visibility into foreign threat actors and nation-state campaigns; the ability to detect patterns of cyber activity across jurisdictions that no single state could see on its own; and a hub-and-spoke information-sharing architecture, anchored by the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), that has allowed real-time warnings, coordinated defense, and rapid response. Robust investment in cybersecurity and information sharing across federal, state, and local governments over the past decade is a major reason that recent federal election cycles have been secure.

But just as the threat environment is poised to accelerate at an exceptional rate, the federal government has dramatically pulled back. Over the past year, CISA has lost more than a third of its workforce, federal funding for the MS-ISAC and EI-ISAC has been eliminated, key grant programs have been conditioned in ways that effectively block access to cybersecurity support,

and longstanding institutional knowledge and relationships have been lost. The result is a widening gap between rapidly escalating threats and diminished federal capacity to help state and local governments meet them.

My testimony today will make four main points. First, cyber attacks on state and local governments can cause significant real-world harm by exposing sensitive personal information and disrupting critical services. Second, AI is poised to exacerbate the structural challenges that SLTT governments have long faced in defending these systems. Third, the federal government's retreat from its traditional supporting role has already produced concrete harms and threatens to produce many more. Fourth, the federal government should act now to restore funding and capabilities, strengthen information sharing, and reaffirm the shared responsibility that has defined federal–state cybersecurity cooperation.

I. Intrusions into State and Local Government Systems Can Harm People by Exposing Sensitive Personal Information and Disrupting Critical Services.

A. State and Local Governments Hold Vast Amounts of Sensitive Personal Information.

SLTT governments, and the vendors who serve them, hold extraordinary volumes of personal information about Americans. In many respects, this information is even more sensitive than what private companies hold about their consumers. Governments collect this information not because people have chosen to share it in a commercial transaction, but because they must do so to access essential services, exercise their rights, or comply with the law. Key categories of personal data include the following:

1. General Administrative Data and Public Benefits.

States collect a wide variety of personally identifiable information through public benefit and service programs—ranging from Medicaid to SNAP to unemployment insurance.[1] While the specifics vary by state and program, this data routinely includes demographic information such as race, sex, gender, disability status, and citizenship; contact information and home addresses;

[1] See Ctr. for Democracy & Tech., The Leadership Conf. Ctr. for Civil Rights and Tech, & Protect Democracy, *Federal Efforts to Expand Access to Data from State-Run Programs and Individual Privacy* (July 23, 2025), https://cdt.org/wp-content/uploads/2025/07/Federal-Efforts-to-Expand-Access-to-Data-from-State-Run-Programs-and-Individual-Privacy-FINAL.pdf.

records of significant life events including job loss, employment history, marriage, and divorce; medical records and health information; and unique identifying details like Social Security numbers. Taken together, this information offers a comprehensive portrait of a person's family, finances, health, and movements.

2. Voter Data.

Voter registration files are large repositories of personal information collected as a condition of exercising the most fundamental right of citizenship.[2] The precise contents of these files vary across states, but at a minimum they typically include a voter's name, residential address, and identifying details such as full or partial Social Security numbers, driver's license numbers, or state identification numbers.

3. Education Data.

State and local education agencies collect particularly sensitive information about children.[3] Education records can include student demographic information, home addresses, academic performance, disciplinary actions, disability status, health information, and—as CDT has documented in its work on immigrant K-12 students—data points such as place of birth, family demographics, and the number of years a student has attended school in the United States.[4] Because this information concerns minors and is generated in the context of compulsory education, the privacy and security stakes are especially high.

The aggregation of administrative, voter, and education data inside state and local systems means that a successful intrusion at the state or local level can yield a richer, more harmful set of information than a comparable breach in many private-sector contexts.

---

[2] See Ctr. for Democracy & Tech., The Leadership Conf. Ctr. for Civil Rights and Tech, & Protect Democracy, *How Federal Efforts to Access Voter Data Affect Our Privacy, Civil Liberties, and Democracy* (Dec 12, 2025), https://cdt.org/wp-content/uploads/2025/12/How-Federal-Efforts-to-Access-Voter-Data-Affect-Our-Privacy-Civil-Liberties-and-Democracy-final.pdf.

[3] Future of Privacy Forum, *Student Privacy Primer* (Oct. 2021), https://fpf.org/wp-content/uploads/2026/04/2_Student-Privacy-Primer_Final6.pdf.

[4] Kristin Woelfel, *Unique Civil Rights Risks for Immigrant K-12 Students on the AI-Powered Campus, Ctr. for Democracy & Tech.* (Jan. 15, 2025), https://cdt.org/insights/brief-unique-civil-rights-risks-for-immigrant-k-12-students-on-the-ai-powered-campus/.

B. State and Local Governments Face Serious Structural Cybersecurity Challenges.

The sensitivity and concentration of personal data make SLTT systems a natural target for hackers. Unfortunately, state and local governments have also historically faced significant structural challenges in defending against cyber threats, and those challenges are growing more acute.

Many state and local governments face persistent funding and workforce constraints that affect their ability to prepare proactively for attacks and to respond efficiently when those attacks occur. Cybersecurity capabilities vary significantly from one locality to another, depending on leadership, budgets, and organizational capacity. Some agencies have deployed advanced defenses and applied strong cyber-hygiene protocols, while others operate with minimal safeguards, sometimes lacking even basic protections such as multi-factor authentication or regular patching.[5] One survey found that more than half of SLTT agencies were below their target cybersecurity maturity level.[6]

States and local jurisdictions, which often lack the resources to recruit and retain in-house cybersecurity talent, are particularly dependent on federal support and expertise, especially at a moment when many states are confronting serious budget pressures. In a recent national survey, state Chief Information Officers cited insufficient cybersecurity budgets and inadequate cybersecurity staffing as two of the top five barriers to addressing cybersecurity challenges in their states.[7]

These challenges are further compounded by the reliance of state and local governments on third-party contractors that process and handle sensitive data on the government's behalf. The security posture of those contractors is often opaque to the people whose data is at stake and, in many cases, to the officials nominally responsible for oversight. When a major contractor is compromised, the consequences can ripple across many states at once.

---

[5] David Kertai, *Improving State and Local Government Cybersecurity, Info. Tech. & Innovation Found.* (Apr. 27, 2026), https://itif.org/publications/2026/04/27/improving-state-local-government-cybersecurity/.

[6] Multi-State Information and Analysis Center, *Nationwide Cybersecurity Review 2024 Summary Report*, https://learn.cisecurity.org/NCSR-summary-report-2024.

[7] Meredith Ward & Mike Wyatt, *2026 NASCIO-Deloitte Cybersecurity Study* (2026), Deloitte Center for Government Insights, https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/2026-nascio-deloitte-cybersecurity-study.html.

C. Recent Incidents Illustrate the Real-World Harms from Cyber Intrusions.

SLTT governments have suffered a steady stream of breaches and service disruptions with concrete, real-world consequences. Many of these breaches disclosed personally identifiable information of millions of people, exposing them to risks such as identity theft, financial fraud, targeted phishing attacks, and takeover of email or social media accounts. For example, in early 2025, the major government services contractor Conduent—which provides processing support for state benefits programs—suffered a data breach that exposed personal data of more than 25 million people.[8] A major breach at student information system provider PowerSchool leaked personal data for more than 10 million teachers and 60 million students.[9] Earlier this year, the breach of the Canvas learning management platform not only disrupted essential learning activities for schools around the country, but exposed sensitive information of over 275 million users, including private messages that may contain deeply personal communications.[10] The risk to schools is widespread: in CDT's 2025 polling on AI in education, 23 percent of teachers in grades six through twelve reported that their school experienced a large-scale data breach in the 2024–25 school year.[11]

Cyber incidents can also lead to disruption of critical services. Recent local incidents underscore that these are not abstract risks. A ransomware attack in Dallas disrupted a range of systems from emergency dispatch to municipal courts.[12] Several Connecticut local governments were forced to shut down networks in response to a ransomware attack.[13] Foster City, California, saw a range of government services taken offline by a cyber attack.[14] In Winona County, Minnesota, residents

---

[8] Zack Whittaker, *Conduent Data Breach Grows, Affecting at Least 25M People*, TechCrunch (Feb. 24, 2026), https://techcrunch.com/2026/02/24/conduent-data-breach-grows-affecting-at-least-25m-people/.

[9] Briana Mendez-Padilla, *Ransomware attacks in education jump 23% year over year*, K-12 Dive (July 21, 2025), https://www.k12dive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/753483.

[10] Jason Koebler, *"The Biggest Student Data Privacy Disaster in History": Canvas Hack Shows the Danger of Centralized EdTech*, 404 Media (May 2026), https://www.404media.co/the-biggest-student-data-privacy-disaster-in-history-canvas-hack-shows-the-danger-of-centralized-edtech/.

[11] Elizabeth Laird, Maddy Dwyer & Hannah Quay-de la Vallee, *Hand in Hand: Schools' Embrace of AI Connected to Increased Risks to Students*, Ctr. for Democracy & Tech. (Oct. 8, 2025), https://cdt.org/insights/hand-in-hand-schools-embrace-of-ai-connected-to-increased-risks-to-students/.

[12] Keely Quinlan, *Dallas ransomware attack compromised data of 30,000 people , officials say*, StateScoop (Sept. 25, 2023), https://statescoop.com/dallas-ransomware-attack-cyberattack-data/.

[13] Mary Ellen Godin, *Connecticut Cyber Incidents Highlight Risk for Local Government*, GovTech (Mar. 10, 2026), https://www.govtech.com/security/connecticut-cyber-incidents-highlight-risk-for-local-govt.

[14] Gillian Mohney, *Cyber Attack Continues to Paralyze Foster City, Calif.*, GovTech (Mar. 24, 2026), https://www.govtech.com/security/cyber-attack-continues-to-paralyze-foster-city-calif.

lost access to DMV and vital-statistics services after a ransomware incident.[15] Each of these episodes meant real people unable to renew a driver's license, obtain a birth certificate, or access local services on which they depend.

D. The Public Is Deeply Concerned About the Privacy and Security Risks to Personal Data Held by Government Agencies.

CDT's recent polling confirms that the American public is acutely aware of these risks and is asking for stronger protections. Three in four Americans are concerned about the privacy and security of the personal data that government agencies collect and store about them—a concern that holds steady across demographic groups, regions, and party lines.[16] More than 80 percent of Americans say that having legal protections for the sensitive information that government agencies collect and store about them is important, and 83 percent are specifically concerned that a data breach of a government database could allow their personal data to be misused.[17] As a result of these concerns, 79 percent of Americans agree that Congress should use its authority to hold government agencies accountable when they ignore privacy laws that protect personal data.[18]

II. Artificial Intelligence Is Accelerating the Cybersecurity Risks Facing State and Local Governments.

Cybersecurity threats are intensifying because of the rapid advance of artificial intelligence. AI is a transformative technology with enormous potential benefits, including for cybersecurity defense. But the same capabilities that make AI useful for defenders also make it a powerful tool for attackers, and the offensive threats are evolving more quickly than most state and local governments can adapt.

---

[15] Gavin Michaelson, *Cyber Attack Impacts DMV, Vital Stats in Winona County, Minn.*, GovTech (Apr. 13, 2026), https://www.govtech.com/security/cyber-attack-impacts-dmv-vital-stats-in-winona-county-minn.

[16] Elizabeth Laird, Maddy Dwyer & Quinn Anex-Ries, *Common Concern: Americans Worried About Personal Data Held by Public Agencies and Want Government Accountability*, Ctr. for Democracy & Tech. (Mar. 31, 2026), https://cdt.org/insights/common-concern-americans-worried-about-personal-data-held-by-public-agencies-and-want-government-accountability/.

[17] *Id.*

[18] *Id.*

A. AI Is Lowering the Barrier to Offensive Cyber Operations.

Increasingly capable AI systems are being used to discover and exploit vulnerabilities in software and networks. The recent announcement of the Mythos Preview from Anthropic underscores how rapidly the frontier is shifting. According to Anthropic's own description, advanced models like Mythos can enable users—including those without deep security expertise—to identify and exploit even sophisticated vulnerabilities.[19] The United Kingdom's AI Safety Institute, in its independent evaluation of the Mythos Preview, found that the model was able to execute multi-stage attacks that would otherwise take human operators days, and to discover and exploit vulnerabilities autonomously. The Institute concluded that the model is particularly capable of attacking small, weakly defended, and vulnerable systems where access to a network has been gained.[20] The Institute subsequently found that OpenAI's GPT-5.5 "reaches a similar level of performance on our cyber evaluations."[21]

State and local agencies often operate the small and weakly defended systems that frontier AI models are best positioned to attack. Anthropic shared the Mythos Preview with a limited set of partners through its Glasswing program in an effort to contain its potential impact, though it is unclear whether or how many SLTT governments are currently included in the program.[22] OpenAI has made GPT 5.5 Cyber available through its Trusted Access for Cyber program, which is open to state and local government defenders.[23] But even where SLTT agencies can access advanced models, state and local cybersecurity teams are already stretched thin and may not be in a position to remediate the vulnerabilities they help to identify. Absorbing a surge in newly discoverable vulnerabilities, along with a corresponding spike in active exploitation as these models and capabilities become available to attackers, poses a challenge to all sectors, and SLTT governments may uniquely struggle given their saturated capacity, often limited resources, and heightened targeting.

---

[19] Anthropic, *Mythos Preview*, https://red.anthropic.com/2026/mythos-preview/.

[20] UK AI Safety Inst., *Our Evaluation of Claude Mythos Preview's Cyber Capabilities* (Apr. 13, 2026), https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities.

[21] UK AI Safety Inst., *Our Evaluation of OpenAI's GPT-5.5 Cyber Capabilities* (Apr 30, 2026), https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities.

[22] Anthropic, *Glasswing Partner Program*, https://www.anthropic.com/glasswing.

[23] OpenAI, *Cybersecurity in the Intelligence Age* (Apr. 2026), https://cdn.openai.com/pdf/7ca95dce-4424-4b62-9eab-89233bb38f82/oai-cybersecurity-action-plan.pdf.

B. AI Adoption Within Government Introduces Its Own Risks.

SLTT governments are also adopting AI for their own use to build software, interact with constituents through chatbots, and analyze data. Each of these uses can deliver important benefits, but also presents new risks. AI-assisted coding, in which non-expert staff use AI to generate production code, can introduce new security vulnerabilities if not subjected to rigorous review.[24] The use of AI to handle and analyze sensitive information creates additional opportunities for data leakage, including the inadvertent regurgitation of training data, the re-identification of de-identified records, and unauthorized access to data sets used to train or fine-tune models.[25] As governments increasingly deploy chatbots and generative AI tools to allow the public to interact with government agencies, the attack surface grows as those bots are connected to ever more data. It can be extraordinarily difficult to design data flows that prevent AI systems from incorporating sensitive information they have ingested into outputs available to users who would not otherwise have access.[26]

The combination of accelerating offensive capabilities, expanding AI deployment, and limited defensive expertise increases the cybersecurity risks that SLTT governments face.

III. Diminished Federal Support Has Significantly Impeded SLTT Cybersecurity Defenses.

For more than a decade, the federal government has supplied a foundational layer of cybersecurity support to state and local governments. That layer has now been substantially eroded, and the consequences are already visible.

A. What the Federal Government Has Provided.

Federal cybersecurity support for state and local agencies has taken several interlocking forms. CISA has supported SLTT cybersecurity by facilitating information sharing of various kinds; deploying advisors who connect federal and local officials; offering red-team services and

---

[24] Will McCurdy, *Vibe Coding Is Causing 'Thousands' of Data Security Vulnerabilities*, PCMag (May 9, 2026), https://www.pcmag.com/news/vibe-coding-is-causing-thousands-of-data-security-vulnerabilities-says.

[25] Ctr. for Democracy & Tech., *Comments to OMB on Federal Agencies' Use of Commercially Available Information* (Dec. 16, 2024), https://cdt.org/wp-content/uploads/2024/12/CDT-FINAL-Comment-re-OMB-CAI-RFI_December-2024.pdf.

[26] *Id*; Anthony Cuthbertson, *'AI gave me your number': The new trend turning ChatGPT hallucinations into harassment*, The Independent (May 10, 2026), https://www.the-independent.com/tech/ai-doxxing-gemini-hallucination-google-b2973008.html.

incident response support; providing curated feeds of threat intelligence; and funding no-cost cyber defense tools—such as Albert sensors that monitor for network intrusions and malicious-domain blocking tools—that officials have described as irreplaceable.[27] These tools have not only protected election infrastructure; in many counties, they have protected the entire county network, on which hospitals, utilities, courts, and emergency services often depend.[28] For many under-resourced jurisdictions around the country, the cybersecurity assistance that CISA provides has been the only source of network-hardening support available. In Washington State, for example, 15 county governments received endpoint security and malicious-domain blocking tools from CISA that secure their network defenses across the entire county government network.[29]

Information sharing is a critical piece of support the federal government has provided to SLTT governments. Such information includes intelligence about potential threat actors and their objectives, tactics, and likely targets; technical indicators and defensive data such as malicious IP addresses and domains; information about known vulnerabilities that malicious actors could exploit; and practices that can improve resilience. In some cases, the federal government is the only actor that can provide this information. Federal intelligence and security agencies have unique visibility into nation-state and other foreign threats, cross-jurisdictional cyber campaigns, and national patterns which no single state or jurisdiction can see in full.

This information is of particular importance for defending critical infrastructure. U.S. election infrastructure, for example, has been a target of foreign governments, whose attacks have escalated in scale and complexity.[30] During the 2024 election, foreign adversaries targeted state and local elections offices using a variety of techniques, including probes of network defenses,[31]

---

[27] Colin Wood, *Secretaries of State Ask DHS to Retain Essential Election Security Services*, StateScoop (Feb. 24, 2025), https://statescoop.com/secretaries-of-state-ask-dhs-to-retain-essential-election-security-services/.

[28] Tim Harper & Isabel Linzer, *Countdown to the Midterms: Mapping the Rapid Evolution of Election Security*, Ctr. for Democracy & Tech. (Feb. 13, 2026), https://cdt.org/insights/countdown-to-the-midterms-mapping-the-rapid-evolution-of-election-security/.

[29] Wash. Sec'y of State, *Letter on CISA and ISAC Funding* (Feb. 2025), https://www.sos.wa.gov/sites/default/files/2025-02/CISA%20and%20ISAC%20Funding%20Letter.pdf.

[30] Vassilis Ntousas & David Salvo, *Democracy in the Crosshairs: Five Key Trends Driving Foreign Interference in Democracies*, German Marshall Fund (Oct. 10, 2024), https://securingdemocracy.gmfus.org/democracy-in-the-crosshairs-five-key-trends-driving-foreign-interference-in-democracies/.

[31] Microsoft Threat Analysis Ctr., *Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024* (Oct. 23, 2024), https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-iran-and-china-continue-influence-campaigns-in-final-weeks-before-election-day-2024.

distributed denial-of-service (DDoS) attacks,[32] and ransomware.[33] An ineffective cybersecurity information-sharing environment leaves state and local jurisdictions on their own, facing sophisticated nation-state adversaries and criminal organizations without the benefits of collective defense.

Another pillar of federal support has been the Information Sharing and Analysis Center (ISAC) ecosystem. ISACs are non-federal organizations that serve as communities of interest sharing cybersecurity information within a sector. The MS-ISAC, operated by the Center for Internet Security, has long focused on the cyber defense of state, local, tribal, and territorial governments.[34] The EI-ISAC, which was originally established as a pilot within the MS-ISAC after election infrastructure was designated critical infrastructure, has grown to include more than 3,700 state and local election offices and has distributed sophisticated intrusion-detection sensors to more than 1,000 election offices around the country.[35] CISA funded these ISACs through cooperative agreements for many years, recognizing that an ISAC operating independently of the federal government plays a uniquely valuable role: it can serve as a more neutral space, insulated from federal political dynamics, and act as a translator between communities that do not always share the same technical or institutional language.

The Department of Homeland Security has also provided grants to SLTT governments to support cybersecurity efforts. The State and Local Cybersecurity Grant Program (SLCGP) has helped eligible entities address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, SLTT governments.[36] The Homeland Security Grant program has provided states and local governments with support to enhance preparedness against evolving threats,

---

[32] Joao Tome & Jocelyn Woolbright, *Exploring Internet Traffic Shifts and Cyber Attacks During the 2024 U.S. Election*, Cloudflare (Nov. 6, 2024), https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/.

[33] FBI, Public Service Announcement, *Just So You Know: Ransomware Disruptions during Voting Periods Will Not Impact the Security and Resiliency of Vote Casting or Counting* (Aug. 15, 2024), https://www.ic3.gov/PSA/2024/PSA240815.

[34] Ctr. for Internet Sec., *MS-ISAC Charter*, https://www.cisecurity.org/ms-isac/ms-isac-charter.

[35] Ctr. for Internet Sec., *EI-ISAC 2018 Year in Review*, https://www.cisecurity.org/wp-content/uploads/2019/02/EI-ISAC-2018-YIR.pdf; DHS Off. of Inspector Gen., *DHS Improved Election Infrastructure Security, but Its Role in Countering Disinformation Has Been Reduced*, OIG-24-52 (Sept. 17, 2024), https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-52-Sep24.pdf.

[36] CISA, *State and Local Cybersecurity Grant Program*, https://www.cisa.gov/cybergrants/slcgp.

including cybersecurity.[37] These grant programs historically have helped state and local agencies purchase cybersecurity tools, update equipment, and harden networks.

In aggregate, the services and funding provided through CISA and the ISACs have enabled the rapid identification of patterns of cyber behavior affecting or endangering SLTT systems; supported bi-directional information sharing; and provided monitoring, warning, and incident response functions that smaller jurisdictions could never independently sustain. CISA's services have also included access to the .gov top-level domain, made available at no cost to qualifying government organizations—an important defense against impersonation and spoofing.[38]

B. Much of That Federal Support Is Now Gone.

Since last February, CISA has cut more than a third of its workforce[39] and eliminated all funding to the MS-ISAC and EI-ISAC.[40] The rollback of CISA and ISAC resources has further kneecapped state and local agencies' ability to stay on top of emerging threats, proactively safeguard their systems, and effectively respond when cyber incidents occur.

The contrast between 2024 and 2025 is illustrative. In 2024, when more than 100 bomb threats tied to Russian-linked actors targeted polling places nationwide, CISA and the EI-ISAC leveraged intelligence-sharing systems and a real-time operations center to alert officials in advance, helping ensure minimal disruption to voting.[41] In 2025, when bomb threats again targeted polling places—this time in New Jersey on Election Day—CISA issued no public guidance and did not activate its real-time operations center. Election officials were left without the situational awareness that had made such a difference the year before.[42]

---

[37] FEMA, *Homeland Security Grant Program*, https://www.fema.gov/grants/preparedness/homeland-security.

[38] CISA & FBI, *The .gov Domain: Helping Mitigate Election Office Cybersecurity and Impersonation Risks* (Apr. 2024), https://npr.brightspotcdn.com/9c/4e/26fe876d40879b4cb186781b6f13/cisa-fbi-the-gov-domain-helping-mitigate-election-office-cybersecurity-and-impersonation-risks-v2-508c.pdf.

[39] Eric Geller, *CISA Workforce Cut by Nearly One-Third So Far*, Cybersecurity Dive (June 4, 2025), https://www.cybersecuritydive.com/news/cisa-departures-trump-workforce-purge/749796/.

[40] Jessica Lyons, *Feds Cut Funding to Program That Share Cyber Threat Info with Local Governments*, The Register (Sept. 30, 2025), https://www.theregister.com/on-prem/2025/09/30/cisa-kills-agreement-with-nonprofit-that-runs-ms-isac/764252.

[41] Jessica Huseman, Jen Fifield, Hayley Harding, Carter Walker, Natalia Contreras & Alexander Shur, *Election Officials Fear Impact of Trump's Cuts to CISA Cybersecurity Agency*, Votebeat (Feb. 28, 2025), https://www.votebeat.org/2025/02/28/cisa-election-cybersecurity-homeland-kristi-noem/.

[42] Patrick Howell O'Neill, *U.S. Elections Face Security Test as DHS Cuts Local Cyber Support*, Bloomberg (Nov. 3, 2025), https://www.bloomberg.com/news/articles/2025-11-03/us-elections-face-security-test-as-dhs-cuts-local-cyber-support.

The damage is not limited to operational capacity. The federal government, and by extension SLTT partners, have lost years of institutional knowledge and expertise about cyber threat monitoring and response. As Republican Secretary of the Commonwealth of Pennsylvania Al Schmidt has observed, CISA brings "a national and global perspective when it comes to cybersecurity risks and all the rest that each individual state can't do on its own."[43] Removing free access to cyber defenses leaves local governments vulnerable to ransomware and other attacks that affect elections, emergency services, schools, hospitals, and far more.

After the loss of federal funding for the EI-ISAC and MS-ISAC, both organizations have shifted to a paid membership model. They are expected to lose roughly two-thirds of the local, state, territorial, and tribal government members they previously served—precisely the smaller and under-resourced jurisdictions that needed them most.[44] As a result, election officials have lost access to critical information shared across jurisdictions, leaving them less prepared and less able to respond effectively to incidents.

Recent guidance has imposed new conditions on federal grants administered by the Department of Homeland Security, further limiting access to cybersecurity support. The HSGP now requires states to demonstrate compliance with the U.S. Election Assistance Commission's Voluntary Voting System Guidelines 2.0—guidance the Administration has separately sought to use to decertify certain voting machines[45]—and to verify that all poll workers are U.S. citizens through the SAVE system.[46] States unable to meet these new requirements have had their election funds withheld. The SLCGP, for its part, has issued new guidance that prohibits states from using grant funds to participate in the EI-ISAC or MS-ISAC, which CISA has stopped funding directly.[47] As a consequence, some states, including Maine, have refused to accept federal cybersecurity funds altogether rather than comply with the new restrictions, forfeiting roughly $130,000 in additional

---

[43] Jordan Wilkie, *Election Officials in Pa. Sound Alarms over Trump's Cuts to Election Security Agencies*, WESA (Feb. 25, 2025), https://www.wesa.fm/politics-government/2025-02-25/trump-election-security-cuts-pennsylvania.

[44] Eric Geller, *Federal Cuts Force Many State and Local Governments Out of Cyber Collaboration Group*, Cybersecurity Dive (Oct. 1, 2025), https://www.cybersecuritydive.com/news/ms-isac-loses-federal-funding-cyber-impacts/761367/.

[45] Verified Voting, *Executive Order Analysis* (Apr. 2025), https://verifiedvoting.org/blog-executive-order-apr-2025/.

[46] FEMA, *FY25 Homeland Security Grant Program Notice of Funding Opportunity*, https://www.fema.gov/grants/preparedness/homeland-security/fy-25-nofo.

[47] Grants.gov, *State and Local Cybersecurity Grant Program FY25 Guidance*, https://grants.gov/search-results-detail/360215.

cybersecurity support.[48] The combined effect is a system in which states are losing direct federal support, losing the option to use what funding remains to participate in the ISACs that previously filled the gap, and in some cases concluding that the conditions on remaining funds make them not worth accepting.

C. Loss of Trust Between SLTT Officials and the Federal Government.

The federal government's actions over the past year have led to the breakdown in trust with state and local officials, particularly with respect to election cybersecurity. As the federal retreat has deepened, the working relationship between state election officials and Washington has frayed. Some officials have stopped using the cybersecurity services CISA still offers, including physical and cybersecurity assessments, because they fear that information shared during those assessments could later be used to pressure or malign their offices.[49]

A particularly striking example occurred when suspected Iranian-linked hackers targeted systems in Arizona this past summer. State officials chose not to report the incident to CISA, citing distrust in how the agency would handle sensitive vulnerability information.[50] That kind of hesitation can have severe consequences. Ransomware and DDoS attacks against local governments have continued to rise—one recent industry analysis reported a 65 percent surge in ransomware attacks on government agencies in 2025[51]—and during a major incident, every hour that information is not shared can translate directly into expanded harm.

The breakdown in the federal–state cybersecurity relationship will be extremely difficult to repair. Officials have expressed concern that the relationship with CISA built over years of careful and diligent work may be permanently damaged, even if support were to return. That outcome becomes more likely with every additional month of erosion. An earlier draft of the Homeland Security appropriations bill for FY2026 would have earmarked CISA funding to

---

[48] Miles Parks, *Trump's DHS Ties Election Security Grants to Voting Policy*, NPR (Aug. 22, 2025), https://www.npr.org/2025/08/22/nx-s1-5508345/election-security-grants-trump-voting-policy.

[49] Kevin Collier, *Less Staff, Even Less Trust: States Say They Can't Rely on Trump's DHS for Election Security*, NBC News (Aug. 1, 2025), https://www.nbcnews.com/tech/security/less-staff-even-less-trust-states-say-cant-rely-trumps-dhs-election-se-rcna220855.

[50] Derek B. Johnson, *After Website Hack, Arizona Election Officials Unload on Trump's CISA*, CyberScoop (July 21, 2025), https://cyberscoop.com/arizona-secretary-of-state-website-hack-candidate-portal-criticizes-cisa/.

[51] Industrial Cyber, *Comparitech Reports 65% Surge in Ransomware Attacks on Government Agencies in 2025*, https://industrialcyber.co/threats-attacks/comparitech-reports-65-surge-in-ransomware-attacks-on-government-agencies-in-2025/.

rehire ten regional election security advisors and fully funded the EI-ISAC at 2024 levels. A return of that support would be a meaningful first step. But Congress, and CISA, will need to do considerably more to rebuild what has been lost.

IV. Recommended Steps Forward

The federal government plays a unique and important role in supporting state and local cybersecurity for at least three reasons. First, much of the data held by SLTT agencies is collected in response to federal mandates. If the federal government requires SLTTs to collect sensitive information, it bears a corresponding responsibility to help ensure that data is protected. Second, the federal government is uniquely positioned to maximize the value of taxpayer dollars spent on cybersecurity. Cybersecurity is an area in which resource and information sharing produces dramatically better outcomes than independent state-by-state efforts; foundational federal support avoids duplication and improves shared threat awareness. Third, states are increasingly the target of nation-state attacks, which they are ill-equipped to handle given the asymmetry of resources and expertise and which raise national security concerns the federal government alone can fully address.

CDT respectfully urges the Committee to support and pursue the following steps:

A. Restore and Stabilize CISA and ISAC Funding.

Congress should restore funding to CISA and the ISAC ecosystem—particularly the MS-ISAC and EI-ISAC—at levels sufficient to rebuild lost workforce capacity, reactivate suspended programs, and re-establish the free or low-cost services on which thousands of state and local jurisdictions have come to rely. The ISACs deserve particular attention as essential intermediaries during a period when trust in direct CISA engagement has been damaged. As neutral, non-federal entities, ISACs can continue to serve communities that have, at least for now, become reluctant to engage directly with the federal government.

Funding for cybersecurity should also be more stable than it has been historically. Programs that depend on year-to-year uncertainty are difficult to staff and difficult to trust. Multi-year support and durable grant models would foster sustained security programs across SLTT sectors. Information-sharing models in particular require stability to build trust, establish partnerships, and deliver lasting security value. Future funding for SLTT cyber information sharing should

focus on longer-term stability and enduring program-building. These stable funding models are especially beneficial to smaller jurisdictions that have fewer resources and greater difficulty attracting cybersecurity expertise.

B. Reinvigorate the Federal Commitment to Information Sharing.

Congress should expressly reaffirm the federal government's commitment to bidirectional information sharing with state and local governments. That includes restoring the operational capacity at CISA to issue timely public guidance during incidents, activating real-time operations centers during high-risk periods such as elections, and providing SLTT partners with consistent, trustworthy points of contact. Restoring those mechanisms will also require concrete actions to rebuild trust, including clear assurances that information shared with the federal government for defensive purposes will not be repurposed in ways that disadvantage state and local officials.

C. Restore and Maintain Funding to SLTT Governments for Privacy and Cybersecurity Protections.

Particularly in the context of AI-driven vulnerability discovery and exploit development, state and local governments will need ready access to the tools and capabilities that allow them to discover and remediate technical vulnerabilities in their systems. CISA and the MS-ISAC and EI-ISAC previously provided vulnerability scanning, red-teaming, and penetration testing at low or no cost. Restoring those capabilities and ensuring they are extended to state and local governments at scale will be essential to closing vulnerabilities across government networks before they are exploited at speed by AI-enabled adversaries.

Congress should also renew the SLCGP and revisit recent grant-program conditions that effectively block states from using federal cybersecurity dollars to participate in the ISACs or that have led some states to refuse cybersecurity funding altogether. Conditions on federal cybersecurity funds should be designed to maximize the security of state and local systems, not to advance unrelated policy objectives at the expense of cybersecurity.

Conclusion

State and local governments are on the front lines of an evolving cyber threat landscape in which artificial intelligence is increasing the risks. They hold extraordinarily sensitive information about Americans and operate systems on which constituents depend for the most basic functions

of daily life. They face structural resource and workforce constraints that make it impossible for them to meet these threats alone. And they are confronting all of this at precisely the moment when the federal government—the partner on which they have most relied—has dramatically pulled back.

Congress should restore the funding, the programs, and the institutional capacity that have made federal–state cybersecurity cooperation work, while modernizing those tools to address the unique risks posed by advanced AI. It should reaffirm the federal government's commitment to information sharing with SLTT partners, conduct rigorous oversight of agencies whose retrenchment has left systems and data exposed, and ensure that incident reporting and public accountability keep pace with the threats. None of this requires inventing new institutions. It requires renewing the sense of shared responsibility that has defined federal–state cooperation on cybersecurity.

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