Mark Raymond
Chief Information Officer
State of Connecticut
Past President and Member, NASCIO

Testimony Before the U.S. House Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection Hearing on the State and Local Cybersecurity Grant Program

April 1, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, I am Mark Raymond, Chief Information Officer for the State of Connecticut. As CIO for Connecticut, I am responsible for the technology of thirty-nine executive branch agencies, including applications, digital government, infrastructure and cybersecurity through the Department of Administrative Services' Bureau of Information Technology Solutions. In my role, I also oversee the Connecticut Education Network, which provides networking and internet services to all K-12 public schools in the state, libraries, universities, and over two thirds of the state's municipal governments. I co-chair our cyber security committee that brings together federal, state and local governments, along with private providers of critical infrastructure such as utilities and hospitals to share best practices, emerging issues and ongoing threat management.

I am also a member of the National Association of Chief Information Officers (NASCIO.) NASCIO represents the nation's Chief Information Officers, Chief Information Security Officers, and Chief Privacy Officers and is a leading voice for states as they work to address critical cybersecurity threats, expand digital services to their constituents, and protect resident data.

Like my colleague Alan Fuller, CIO for the State of Utah, I am here before you today to speak about the importance of the State and Local Cybersecurity Grant Program. As a former president of NASCIO and one of the longest tenured state CIOs, I can tell you that states have advocated for a dedicated program such as this for many years. The threats posed to state and local networks by nation-state actors, criminal networks, and natural disasters are numerous and unceasing. Each year, cyber-attacks become more sophisticated and more threatening, and the risk posed to residents become even more dire.

State and local governments serve as stewards of civil society, working to ensure community stability, predictability, and the well-being of the residents we serve. State and local public servants are the teachers in our classrooms, the police officers that respond to distress, the doctors and nurses that care for our neighbors suffering with addiction. They protect the water we drink, the food we eat, and much more. All these services are provided with the assistance of technology that must also guard people's most sensitive data. These services are vital to protect and ensure they can continue to operate safely amidst an ever-increasing set of direct

threats. It is important to note that those who deliver these services often do not have the appropriate funds to adequately protect the technology and data within their care alone.

While states are ready to meet this challenge, it is critical that they receive support from their federal partners if they are to remain effective. The State and Local Cybersecurity Grant Program has already proven to be a valuable resource in meeting this goal. By offering both technology services and direct payments to local governments, states have been able to further the "whole-of-state" approach to cybersecurity that helps to address much of the "low-hanging fruit" of cyber hygiene that many small and rural communities cannot accomplish on their own.

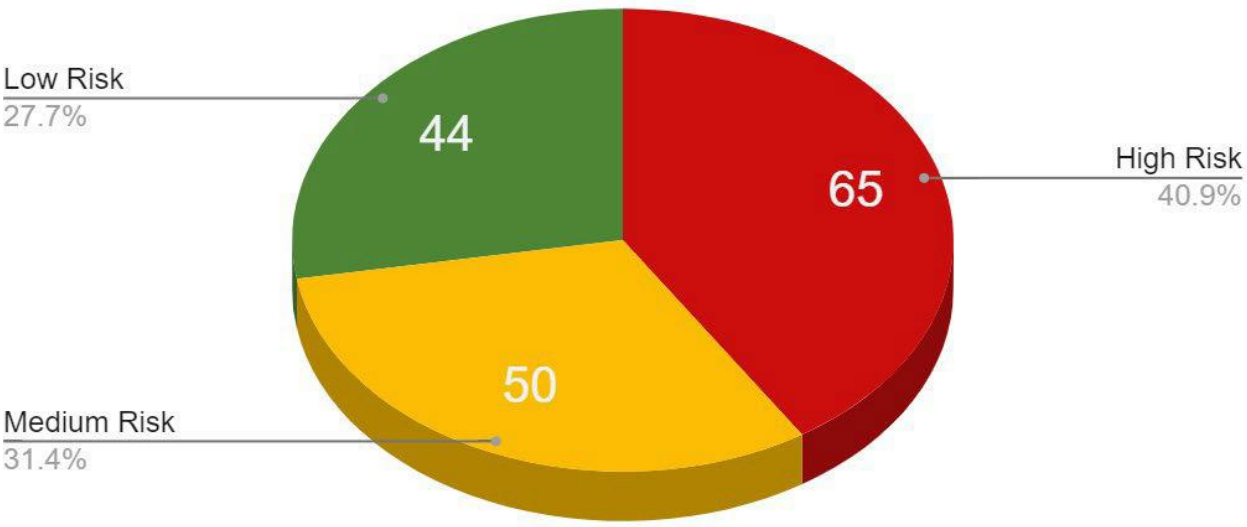
To that end, through the grant, we have expanded state offerings to local governments, including risk assessments, dot gov domain expansion, multi-factor authentication, ransomware prevention software, employee training, and other critical services. Perhaps most important, however, is the spirit of trust and collaboration that the grant has fostered between state and local governments. The process of developing the cybersecurity plan required by CISA to receive grant funding has meant that cyber incident responders and those tasked with protecting critical technology infrastructure are meeting and collaborating *before* attacks take place rather than during or after. Preventing attacks is far better than recovering from them.

Like most of our fellow New England states, Connecticut does not provide government services through a county government structure. Services are only provided at the state or municipal level. The outcome of our structure is that our state government often must fill more gaps than others that provide county services. This makes collaboration and state-level services even more critical to our 169 cities and towns. To illustrate the impact of the SLCGP, I will highlight some specific examples of how we've put this program to work in my state of Connecticut.

Connecticut Experience

For the FY 2022 Grant Program year, we awarded $2,978,432 through the SLGCP, with more than $2.1 million flowing directly to local governments. Awards for the FY 2023 Program Year are currently under development and are expected to provide $6,832,343 in total and $4,372,700 to local governments.

One of the great benefits of the program was a systematic assessment and reporting of risks that our municipalities face. The State of Connecticut proudly partnered with our Connecticut National Guard to evaluate cyber risks using the NIST Cybersecurity Framework, which can be visualized in the following graphic.



Of the 159 municipalities assessed, only 44 (27.7 %) of Connecticut Municipalities were assessed as low risk. The ultimate measure of success of any cybersecurity program is the reduction of risks in a very dangerous online world. The periodic assessments supported by the SLCGP ensure that the actions we take have measurable results.

The areas that primarily contributed to high risk ratings were lack of vulnerability scanning, missing multi-factor authentication, lack of employee cybersecurity training, poor capability malware protection tools, and lack of incident response plans. The SLGCP program awards made in Connecticut will directly address these findings.

Fifty-one total awards were made, of which 19 addressed planning and governance, 31 addressed cyber tool improvements such as multi-factor authentication and ransomware protections, and the remaining award covered training and awareness for the entire community. The top 10 awards went to medium-sized schools and towns that have substantial needs for the population yet insufficient local funding to address the risks sustainably.

Unfortunately, available SLGCP funds for FY 2022 improvements covered less than half of the overall need. We hope to continue these needed improvements utilizing the remaining grant years, and we expect ever increasing demand from our local partners.

Of note was an award to support the Cyber Nutmeg exercise. This effort is a multi-stakeholder collaboration between our Division of Emergency Management and Homeland Security, the Department of Administrative Services, Connecticut National Guard, CISA, and the Connecticut Education Network to support a two-day exercise where all municipalities and critical infrastructure operators are invited to participate. This unique, state-level exercise critically

raises awareness, exercises incident management plans, and improves relationships that are needed when incidents occur.

Next Steps

Though much has already been accomplished under SLCGP, we recognize that more can be done to continue this work. Many local governments have stated that their fear that the program may expire impedes their application for future funding. They are reluctant to go through the arduous task of standing up a new cybersecurity program and acquiring the matching funds needed, only to have federal support evaporate after a few years. Additionally, stabilizing the matching formula across all grant years would help significantly simplify administration and attract more applicants.

For a state like Connecticut, where no county government exists, the administrative effort to demonstrate each locality has signed onto a shared or statewide solution could be reduced. Flexibility to implement shared solutions, such as a statewide Security Operation Center, would better serve states. Such solutions should be funded as a default offering, allowing municipal governments to opt-out. This would establish collaboration as the expectation in reducing cybersecurity risks and, therefore, reducing overall costs.

However, while changes and improvements are needed, we strongly believe that it is better to continue to improve SLCGP rather than allow it to expire. We have no reason to believe that states, towns, schools and critical infrastructure providers will see less targeting by criminals, nation states and cyber activists. Rather, we expect that the threats faced by stakeholders will only increase in the coming years. This grant has helped to establish a solid foundation to continue to expand our nation's cybersecurity defenses. As the current Administration intends to increase the responsibility of state and local government to respond to cyberattacks, it is logical that the federal government provide the tools and resources needed to meet this increased burden.

Thank you for your time today. I look forward to answering your questions.