NATIONAL LEAGUE OF CITIES

A CENTURY OF STRENGTHENING CITIES

STATEMENT OF

THE HONORABLE KEVIN KRAMER

FIRST VICE PRESIDENT, NATIONAL LEAGUE OF CITIES AND

COUNCILMAN, LOUISVILLE METROPOLITAN GOVERNMENT, KENTUCKY

ON BEHALF OF THE NATIONAL LEAGUE OF CITIES

BEFORE THE HOUSE HOMELAND SECURITY COMMITTEE SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION HEARING,

“CYBERSECURITY IS LOCAL, TOO: ASSESSING THE STATE AND LOCAL CYBERSECURITY GRANT PROGRAM”

APRIL 1, 2025

Good morning, Chairman Garbarino, Ranking Member Swalwell, and members of the Subcommittee.

I am Councilman Kevin Kramer from Louisville Metro Government in Kentucky, and First Vice President of the National League of Cities. Thank you for inviting NLC to testify before the subcommittee today as you consider reauthorization of the State and Local Cybersecurity Grant Program. I am pleased to share with you my city's experience as a recipient of one of these grants, as well as the perspective of cities, towns and villages throughout the nation.

The National League of Cities represents cities, towns and villages of all sizes as we work together to ensure a strong federal-local partnership for our country. I am honored to speak as a Councilman for Louisville Metropolitan Government, as well as on behalf of the nation's more than 19,000 cities, towns and villages in each congressional district in the country. Prior to serving as NLC's Vice President, I served as Chair of NLC's Information Technology and Communications Committee. I also am employed as a teacher at a small all-girls high school and am familiar with the cybersecurity capacity limitations of schools.

Local governments are high-priority targets for both criminal organizations and nation-state actors. Municipalities are responsible for sensitive data, payment systems, critical infrastructure, and public services that directly impact the health and safety of residents. Attacks on municipal networks can dangerously hamper emergency response, endanger resident data, bring city services to a halt, and cost cities hundreds of thousands of dollars and hundreds of work hours, if not more, to stop and recover from the damage to city systems. As this committee has noted in previous hearings, local governments of all sizes face serious capacity limitations to prepare for and respond to cyberthreats.

Louisville Metro Government has a population of 622,981, but most municipalities are much smaller. Of the more than 19,000 cities, towns and villages in the country, over 16,000 have populations below 10,000 people. Small communities have correspondingly small budgets and staff. Most municipalities lack a dedicated full-time IT staff member, and those larger communities with full IT departments frequently struggle to attract workers with the appropriate levels of expertise in technology and cybersecurity. However, smaller size does not make a community any less susceptible to attack.

Louisville Metro Government's Perspective

Louisville Metro Government has received awards from the State and Local Cybersecurity Grant Program in two fiscal year cycles. The latest grant awarded allowed our community to do two main things. First, it allowed Louisville Metro Government to perform comprehensive testing of critical systems, such as lifesaving applications, without reliance on third parties which is expensive and can take months to arrange and execute.

Secondly, it allowed Louisville Metro Government to take in and share critical cyber threat information with regional and statewide partners by standing up the Kentucky Cyber Threat Intelligence Cooperative (KCTIC). We are taking on this effort to address the latency of actionable threat information provided by government entities, private security companies, and our regional partners.

We will provide a platform for non-attributable threat information that can be shared in near real time. Experience has shown us that knowing when bad actors are attacking specific vulnerabilities or using particular tactics in our neighboring jurisdictions and local organizations gives us the opportunity to harden our own defenses. We have regional government partners and private companies interested in joining KCTIC. This effort is a grassroots program designed to strengthen the cyber resilience of the region and overcome inefficiencies of many current processes and is directly supported by SLCGP.

Reauthorizing the State and Local Cybersecurity Grant Program

Our nation needs a strong federal-state-local partnership to guard against the rising threat of cyberattack. The State and Local Cybersecurity Grant Program is a crucial pillar in the country's security strategy. The first years of the program have created a pathway for partnership through the development and maintenances of state plans, intergovernmental collaboration through state cybersecurity committees, and increased education and awareness of cybersecurity issues among local leaders. We are beginning to see promising practices, as well as potential areas of improvement for reauthorization.

Funding for local government cybersecurity from multiple sources is crucial, particularly for smaller jurisdictions. Most municipalities have many competing high-priority needs in the community, as well as many limitations on their ability to raise revenues to fund those needs. It is difficult for a small community in need of new water pipes, a fire engine, and street repaving to prioritize budget funds for migration to the .gov domain or implementation of multifactor authentication, despite the security value of those actions. The State and Local Government Cybersecurity Grant Program helps alleviate some of that budget pressure, while also fostering a culture of intergovernmental collaboration and prioritization of cybersecurity within participating states.

But for the SLCGP to reach its full potential, improvements are needed. The one-size-fits-all passthrough model of the SLCGP limits the program's efficiency. Larger jurisdictions such as Louisville Metro Government are well-positioned to apply directly for a competitive federal cybersecurity grant and requiring all municipalities to apply for a state passthrough only increases the amount of public dollars spent on program administration. NLC encourages Congress to create a direct competitive grant fund within the SLCGP for larger municipalities to apply for directly.

Smaller communities across a wide number of states have also raised concerns about both the tight application windows for SLCGP funds and the complexity of the application process. Small towns are poised to benefit the most from cybersecurity funding, yet lack the staff support to manage a complex grant application and administration process. A tight application window exacerbates this problem, as communities need time to assess their needs, scope out and get quotes for solutions to the gaps they identify and complete all required elements of the application. NLC recommends that the application process be simplified to encourage participation by more small communities, while balancing that streamlining with the need to protect the program from waste, fraud and abuse. We are also encouraged by states willing to explore multi-stakeholder grants that benefit many jurisdictions, such as a state municipal association managing grant application as the prime recipient and providing services directly to a large pool of communities within that state. Just as most people take their cars to a qualified mechanic, small governments need trusted partners to handle complex cyber tasks.

Above all, NLC strongly urges Congress to reauthorize and adequately and consistently fund the SLCGP. The tens of thousands of municipalities, counties, and special districts need strong federal partnership to protect the nation's critical infrastructure and the public services that protect residents' health and safety. States and local governments have built the framework of a system to protect against cyberattacks, through developing and maintaining state plans and raising awareness at all levels of government about threats, readiness gaps, and solutions. For this system to become strong and effective, it requires consistency from the federal government from year to year. Without consistent expectation of SLCGP's future availability, local governments are less likely to do the self-assessment and advance planning necessary for a successful grant application when the window opens.

NLC looks forward to supporting the Committee in the reauthorization of the State and Local Cybersecurity Grant Program. Cybersecurity is a whole of nation challenge, and requires a truly intergovernmental partnership between federal, state, and local entities to keep our nation's infrastructure and our residents safe and secure. The State and Local Cybersecurity Grant Program is a crucial piece of this puzzle. Thank you for the opportunity to address you today, and I look forward to your questions.