LMC LEAGUE of MINNESOTA CITIES

Association of Minnesota Counties

November 22, 2024

Re: City and County Cybersecurity Grant Program

Dear Legislative Commission on Cybersecurity Members,

The League of Minnesota Cities and the Association of Minnesota Counties write to ask for your support and feedback on a $20 million budget request for the establishment of a City and County Cybersecurity Grant Program to be administered by Minnesota IT Services. The intent of the program is to build on the momentum of the federally funded and MNIT implemented State and Local Cybersecurity Grant Program (SLCGP) by filling critical gaps for under-resourced cities and counties that lack the hardware and software capacity to directly benefit from the MNIT and Minnesota Cybersecurity Task Force’s Whole-of-State Cybersecurity Plan.

The $18 million of federal SLCGP funding in addition to the $5.5 million in state matching funds passed by the legislature will address high level cybersecurity efforts that will seek to harden and improve cyber defense at the state and local level. However, while the Whole-of-State Cybersecurity Plan is a critical piece of a larger puzzle aimed at securing Minnesota, significant gaps remain for the vast majority of cities and many counties who still lack baseline IT maturity to realize the benefits of the Whole-of-State Cybersecurity Plan. This first tranche of funds is not sufficient to ensure all local entities will have the capabilities to benefit from the plan and key gaps remain for the state’s smallest and least-resourced cities and counties.

With a modest infusion of state general fund resources, a state-run City and County Cybersecurity Grant Program will ensure that the SLCGP dollars go further and that cities and counties regardless of size will have the opportunity to apply for modest grants that will boost their cybersecurity capabilities.

City and County Metrics

Through surveying and analysis, the IT maturity based on city size of all 855 cities have been identified by the League of Minnesota Cities and significant gaps remain that will not be addressed with the limited resources of the SLCGP dollars and the Whole-of-State Cybersecurity Plan. Of the 150 cities with populations above 5,000, 83 employ IT staff or some type of managed service and will stand to benefit the most from the SLCGP resources due to their more sophisticated networks that boast above minimum recommendations for active network management as well as hardware and software capabilities.

The remaining 702 cities do not have dedicated IT staff and on average have 7 total FTEs working for the city with almost one third having 1 FTE or less. These cities have minimal technology and lack minimum hardware and software capabilities including data backup systems and data security, which are critical for a baseline cybersecurity posture. While these cities are small, many manage some sort of critical infrastructure like water and wastewater treatment facilities that have become a target for ransomware attacks. From a city perspective, these are the cities that desperately need expertise and resources to help purchase and set up data backup systems, secure data, and utilize commercial and secure email systems and productivity software which are gaps that remain with the SLCGP funds and would be well served by a state supported grant system.

Minnesota's 87 counties are responsible for an immense amount of information. From criminal justice and law enforcement data to children and family records—as well as health and housing information—counties are on the frontlines of protecting Minnesotans' information and the subject of countless breach attempts every day. But financial resources for needed cybersecurity improvements are difficult to come by.

Small and medium-sized counties are particularly vulnerable to cyberattacks. These counties often have IT departments of less than five employees, many have only one IT employee, and some have no IT staff on-site at all. Yet they must protect sensitive and private information the same as larger and urban counties. A recent survey of county IT leaders showed that medium sized counties like Morrison and Douglas have a backlog of cybersecurity needs in excess of $500,000. Most counties have a moderately strong baseline cybersecurity posture, but lack funding for more advanced systems, hardware, and software that correlates with the level of sensitive and private information they are entrusted with protecting.

Proposed Program Framework

The proposed program would be administered by MNIT with the Commissioner establishing a discretionary grant application and scoring criteria as well as tracking and annual reporting requirements, which would be required of all grantees.

Eligible entities of the proposed state supported city and county cybersecurity grant program would include all cities and counties. Due to the likelihood that a small amount of general fund spending may be available for this program, it is suggested to target only cities and counties with this program. However, the program could be extended in the future to schools with the understanding the schools have a different set of needs than counties and cities.

We suggest that the program employ a tiered non-state match requirement, which would structure the program so that larger cities and counties with more sophisticated needs to advance their cybersecurity capabilities would have a higher match requirement than smaller cities and counties. Larger and better-positioned cities and counties would be required to contribute a 50-75% non-state match amount while the smallest cities and counties for smaller grants would not be required to provide matching funds. Grant amounts could also vary based on population and need with the smallest cities and counties benefitting greatly from smaller grants up to $25,000 to purchase and setup data backup systems among other initiatives. Grants to larger cities and counties with a higher 50-75% matching could be capped at $1 million.

In general, eligible expenditures will be assessed in context of need and focus on reducing overall risk across all local government entities. Investments will be targeted at promoting availability of systems that underpin critical infrastructure and public services, protecting public data, and promoting local government compliance with State Law, executive orders, and industry best-practices.

Eligible expenditures could include the following:

- **General IT Services**
  - Technical consulting support for the configuration and installation of security solutions and systems and managed IT services for system and network management.

- **Hardware and Consultant Services Securing Operational Technology and Industrial Control Systems**
  - Consultant and system integrator support to assess and analyze risk to Critical Infrastructure networks, develop response plans, and manual operations procedures.
  - Network hardware needed to fully segregate and secure Critical Infrastructure from the internet and general office networks.

- **Onsite network storage devices and hardware backup solutions**

- **Cloud-based backup and data storage services**
  - Provide redundant off-site backup capabilities.
  - Protect against ransomware when file immutability (write-once, read-many) features are enabled.

- **File management and data archiving solutions**

- **Managed email hosting and productivity & collaboration software**

- **Email filtering solutions**
  - Allows identification and quarantining of phishing attacks by analyzing domain information and message content for suspicious indicators.

- **Web filtering and DNS solutions**

- **Anti-virus and endpoint detection and response software**

- **Firewalls, network switches, and other networking hardware**