Written Statement for the Record

The Honorable B. Glen Whitley

County Judge, Tarrant County, Texas

On Behalf of the National Association of Counties

for the hearing

"Addressing Emerging Cybersecurity Threats to State and Local Government"

Welcome and Introduction

Chairwoman Hassan, Ranking Member Paul, and Members of the Subcommittee, my name is Glen Whitley and I serve as County Judge for Tarrant County, Texas. I also serve on the Board of Directors as Past President for the National Association of Counties (NACo). It is an honor to participate in today's hearing on behalf of Tarrant County, NACo and our local intergovernmental partners across the country.

As the 15th most populous county in the United States, Tarrant County is a hard cyber target. Our county is probed, scanned, phished, and outright attacked roughly 950 times per hour on a good day. While each county is unique, all county governments share core challenges to serving as stewards of public property, safety, and welfare. My remarks today will not only highlight the specific cyber priorities for Tarrant County, but also the overall challenges facing counties of all sizes.

The New Theater of War

In just the past year, we have seen several cyber exploitations that caused major disruptions across the United States. These attacks – including the Microsoft Exchange exploit, SolarWind's spyware breach, the Colonial Pipeline shutdown, and the JBS meat processing hack – all demonstrate exactly how vulnerable our nation's cyber security infrastructure truly is.

At the local level, we have experienced multiple ransomware attacks in recent years. Pinellas County, Florida, for example, recently experienced an attack on their water treatment facility allowing hackers to boost the level of sodium hydroxide in their water supply. As county reliance on technology increases, these attacks will likely increase as well.

Not only are these attacks endangering national security and costing billions in ransom and repair costs, but they also have a direct and lasting impact on the wallets of our residents. Unfortunately, cyber security experts expect these threats to escalate and possibly correlate with critical government activities like elections and tax collection. Online attacks to domestic

cyber infrastructure are quickly becoming the battlefield of choice for bad actors in the 21st Century.

Restrictions on Resources

To better understand how local governments are able to respond to cyber threats, it is important to start with the underlying challenges to local revenue and resources.

General revenues from local property taxes are the backbone of county funding because they are not restricted to a particular activity. Unfortunately, outmigration in many rural counties is reducing the local tax base while 43 states are imposing some type of limitation on counties' ability to increase local taxes.

Restrictions on federal and state resources also remain a challenge. Locally collected general revenues are not restricted to a particular activity and offer counties the flexibility needed to provide mandated services while addressing the unique needs of their communities. Unfortunately, about 93 percent of the state and federal funding used by county governments is restricted to a specific function. [1]

Matching requirements for federal grant and loan programs also make leveraging federal resources impossible for many counties. Subsequently, counties are increasingly forced to fund mandated services with general revenues and charges.

In recognition of lost revenue due to the COVID-19 pandemic, the American Rescue Plan (ARP) Act included $61.5 billion to county governments. Counties thank Congress for making this historic investment in America's counties. However, the U.S. Treasury prevented local governments from using these ARP dollars as a non-federal match for grant and loan programs. As counties now look for ways to leverage this critical assistance – many federal grant and loan

[1] https://www.naco.org/articles/counties-still-challenged-recession%E2%80%99s-recovery

programs will remain out of reach. Without relieving the pressure on county needs elsewhere, counties will struggle to invest in the cyber security infrastructure they need.

County Roles and Core Cyber Priorities

Counties are responsible for delivering a broad array of programs and services that provide a foundation for strong and stable economies. Collectively, counties own or operate thousands of hospitals, public health departments, water and waste management centers, jails, and emergency operations centers – all of which create significant cyber vulnerabilities. Without robust and reliable funding, these local assets expose our communities and these critical programs and services.

To help centralize assistance and best-practices, NACo's Tech Xchange provides county IT leaders an opportunity to diagnose and dialogue over cyber-related challenges. Additionally, a recent NACo survey found that 40% of counties placed cybersecurity as their #1 challenge for county IT.

It is important to note that cyber security needs are not only driven by exposures and vulnerabilities, but also by counties looking to meet certain national standards such as National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS) controls.

In Tarrant County, we adhere to the core principles of the NIST Cybersecurity Framework (NIST CSF) which are Protect, Detect, Respond & Recover. Achieving and maintaining these core principles requires an Information Security Program (ISP) that includes policies, procedures, and resources. While policies and procedures can be downloaded and customized, resources require continuous funding.

More generally speaking, county cyber resources are typically directed to three main areas – Education and Access, Infrastructure, and Preparedness.

Education and Access

It is regularly stated that an organization's greatest cyber weakness is the end user or employee. This is no different for local governments. A recent Cybersecurity Survey conducted by TalentLMS on behalf of Kenna Security found that 70% of employees polled said they recently received cybersecurity training from their employers, yet 61% failed their basic quiz on the topic.[2] In terms of access, it is a well-known best practice to only grant the level of access that is needed for one to fulfill their responsibilities. Yet, we often hear of cyberattacks that resulted in the bad actor gaining access to the county network because an end user had a higher level of access than they needed. A county of Tarrant County's size would expect to send roughly $50,000 on education and security awareness testing campaigns each year alone.

Infrastructure

One of the most basic best practices in the current environment, is the implementation of multi-factor authentication. Similar many online banking operations, this multi-factor approach is vitally needed in local government. Yet, it is a challenge for many counties to implement, from both an IT resource and cost perspective. Other infrastructure needs include updating and replacing network devices to stay ahead of evolving threats. Further, being able to vet cloud software and infrastructure providers as well as the supply chain requires time, money, and skilled personnel. A typical urban county could expect to spend roughly $200,000 each year on detection and prevention systems.

Preparedness

Preparedness is the county's ability to effectively monitor the threats "knocking" at our doors. This requires either the implementation of costly tools or securing externally managed services to perform the task. Resources such as CISA and the MS-ISAC provide assistance for some of these measures. Finally, preparedness includes the development of security policies and incident procedures, as well as regular testing through cyberattack simulations or "tabletops." Counties need significant guidance, resources, and affordable solutions to implement these

[2] https://www.scmagazine.com/home/security-news/61-percent-of-employees-fail-basic-cybersecurity-quiz/

tools, as well as technical assistance for the development of sound standards. A county could reasonably spend around $100,000 annually on quarterly vulnerability and penetration testing.

In addition to these expenses, a county of Tarrant County's size should also expect to spend roughly $650,000 each year for the manpower needed to manage and maintain all of these operations.

Direct and Flexible Funding

The difficulty leveraging CARES Act dollars to address the COVID-19 pandemic exposed how important direct and flexible funding is for local governments. Congress improved on these challenges through the American Rescue Plan which provided direct resources to America's counties struggling to meet their budgetary needs. As you consider how to best allocate cyber security investments, it is imperative for federal resources to reach their intended targets as quickly as possible.

Understandably, block grants help to quickly move resources out of Washington. However, that does not always translate to efficient or effective dollars. We applaud Chairwoman Hassan's work ensuring that a robust investment in our nation's cyber security infrastructure recognizes the need for direct and flexible resources.

Local governments will carry some of the heaviest burdens to securing our nation's cyber infrastructure. Therefore, it is imperative for local governments to play a significant role in the development of state-wide cyber security plans. This requires a meaningful seat at the table – not just a ceremonial appointment for political allies.

To guarantee these resources reach their intended targets, block grants should also have strict pass-through requirements. Additionally, local governments should have the flexibility to adapt and apply those resources to fit the unique challenges of their communities.

Closing

In closing, counties need a strong federal partner that can provide direct and flexible resources that allow local governments to quickly adapt those resources to meet the unique needs of their communities. This is especially true for cybersecurity resources – local governments own and operate some of our nation's most critical infrastructure. Without dedicated federal resources, many of our counties will remain defenseless to cyber threats and the potential for irreparable harm.