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

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 1, 2025

Serial No. 119–10

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

61–302 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, *Vice Chair*
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona
ANDREW OGLES, Tennessee
SHERI BIGGS, South Carolina
GABE EVANS, Colorado
RYAN MACKENZIE, Pennsylvania
BRAD KNOTT, North Carolina

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
DANIEL S. GOLDMAN, New York
DELIA C. RAMIREZ, Illinois
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
JULIE JOHNSON, Texas, *Vice Ranking Member*
PABLO JOSÉ HERNÁNDEZ, Puerto Rico
NELLIE POU, New Jersey
TROY A. CARTER, Louisiana
ROBERT GARCIA, California
VACANT

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CLAY HIGGINS, Louisiana
CARLOS A. GIMENEZ, Florida
MORGAN LUTTRELL, Texas
ANDREW OGLES, Tennessee
MARK E. GREEN, MD, Tennessee *(ex officio)*

ERIC SWALWELL, California, *Ranking Member*
SETH MAGAZINER, Rhode Island
LAMONICA MCIVER, New Jersey
VACANT
BENNIE G. THOMPSON, Mississippi *(ex officio)*

ALEXANDRA SEYMOUR, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

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

Tuesday, April 1, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:06 a.m., in room 310, Cannon House Office Building, Hon. Andrew R. Garbarino (Chairman of the subcommittee) presiding.

Present: Representatives Garbarino, Luttrell, Ogles, Swalwell, and Magaziner.

Mr. GARBARINO. The Homeland Security sub on Cybersecurity and Infrastructure Protection will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the State and Local Cybersecurity Grant Program, which is up for reauthorization this year. Since Congress signed the program into law 4 years ago nearly 1 billion has been allocated to bolster the cybersecurity postures of State and local governments. Today, we will assess the program strengths and weaknesses as we consider next steps.

I now recognize myself for an opening statement. The threat of cyber attacks to the U.S. networks and critical infrastructure is real and rising. Microsoft's 2024 digital defense report estimates that its customers are targeted with more than 600 million attacks per day from nation-states and criminal actors. For years the intelligence community has warned of the threat of state-sponsored cyber actors engaging in malicious activities against our critical infrastructure. As we've seen, those warnings have become a reality. With the persistent threat that groups like Typhoons pose to IT and OTS, any critical infrastructure sector could be the next to fall victim to attacks or have their status seized through a phishing scheme.

As cyber actors become increasingly sophisticated and persistent we can no longer be complacent when it comes to securing our critical infrastructure. We make take all steps necessary to ensure our Nation's cyber preparedness and resilience.

In doing so, it is essential that our State and local government partners are similarly well-situated to respond to these threats. Despite often lacking resources and qualified talent for cybersecurity, State and local governments host the key pieces of critical infra-

structure that keep our economy running. If left unprotected, this presents a huge vulnerability.

Both State and local governments improve their cybersecurity postures, Congress passed the State and Local Cybersecurity Grant Program in 2021. Since this program began, $838 million has been allocated to address cybersecurity risks and threats to information systems owned and operated by or on behalf of State, local, and territorial governments.

State and Local Cybersecurity Grant Program is set to expire this September, at which point the program will not continue to receive Federal funding unless reauthorized by Congress. As we have heard from many stakeholders, this program has undoubtedly improved, sometimes even established the cybersecurity posture for our States and localities.

I am encouraged by the progress and applaud the efforts of our State and local governments to seize this opportunity to prioritize cybersecurity. With that said, we know the program does not come without its challenges. As we consider reauthorization, we want to understand any administrative burdens or barriers to ensure State, local, and territorial governments can focus on cyber resilience and preparedness. To that end, it is also Congress' responsibility to evaluate whether State and Local Cybersecurity Grant Program is the most efficient and effective means to strengthen the cybersecurity posture State and local and territorial governments.

I'm here with an open mind and vested interest in understanding how the program is working. Cybersecurity is a whole of a society challenge, meaning Federal Government must continue to support and strengthen cybersecurity at the State and local levels to protect our Nation's networks and critical infrastructure.

State and local governments must also continue to share information with each other. They play an important role in disseminating best practices which could greatly benefit organizations with less mature cybersecurity programs.

I want to thank our witnesses. We have all had first-hand experience with the State and Local Cybersecurity Grant Program for being here today. I look forward to hearing your perspectives on the program and working with you to strengthen our collective defense against cyber threats.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

APRIL 1, 2025

The threat of cyber attacks to U.S. networks and critical infrastructure is real and rising. Microsoft's 2024 Digital Defense Report estimates that its customers are targeted with more than 600 million attacks per day from nation-states and criminal actors.

For years, the intelligence community has warned of the threat of state-sponsored cyber actors engaging in malicious activities against our critical infrastructure. As we've seen, these warnings have become a reality. With the persistent threat that groups like the Typhoons pose to IT and OT assets, any critical infrastructure sector could be the next to fall victim to attacks, or have its data seized through a phishing scheme.

As cyber actors become increasingly sophisticated and persistent, we can no longer be complacent when it comes to securing our critical infrastructure. We must take all steps necessary to ensure our Nation's cyber preparedness and resilience. In doing so, it is essential that our State and local government partners are simi-

larly well-situated to respond to these threats. Despite often lacking resources and qualified talent for cybersecurity, State and local governments host the key pieces of critical infrastructure that keep our economy running. If left unprotected, this presents a huge vulnerability.

To help State and local governments improve their cybersecurity postures, Congress passed the State and Local Cybersecurity Grant Program in 2021. Since this program began, $838 million has been allocated to address cybersecurity risks and threats to information systems owned and operated by, or on behalf of, State, local, and territorial governments.

The State and Local Cybersecurity Grant Program is set to expire this September, at which point the program will not continue to receive Federal funding unless reauthorized by Congress. As we have heard from many stakeholders, this program has undoubtedly improved—and sometimes even established—the cybersecurity posture of our States and localities. I am encouraged by the progress and applaud the efforts of our State and local governments to seize this opportunity to prioritize cybersecurity.

With that said, we know that the program does not come without its challenges. As we consider reauthorization, we want to understand any administrative burdens or barriers to ensure State, local, and territorial governments can focus on cyber resiliency and preparedness.

To that end, it is also Congress's responsibility to evaluate whether the State and Local Cybersecurity Grant Program is the most efficient and effective means of strengthening the cybersecurity posture of State, local, and territorial governments. I am here with an open mind—and a vested interest—in understanding how the Program is working.

Cybersecurity is a whole-of-society challenge, meaning the Federal Government must continue to support and strengthen cybersecurity at the State and local levels to protect our Nation's networks and critical infrastructure. State and local governments must also continue to share information with each other. They play an important role in disseminating best practices, which could greatly benefit organizations with less mature cybersecurity programs.

I want to thank our witnesses—who have had first-hand experience with the State and Local Cybersecurity Grant Program—for being here today. I look forward to hearing your perspectives on the program, and to working with you to strengthen our collective defense against cyber threats.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman form California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. Morning, thank you to Chairman Garbarino for holding this subcommittee hearing on State and Local Cybersecurity Grant Programs. I also want to thank our witnesses for their participation, in a nice blend of private-sector and public-sector witnesses that we have today.

This program was established 4 years ago as the product of a bipartisan agreement from this committee. As we consider further authorization, it's important to remember that cyber attacks hit Republican districts and Democratic districts, they are in—they are in blue States and red States, they are in urban areas, suburban areas, and rural areas.

In my district, the 14th District of California in the Bay area, the city of Hayward suffered a ransomware attack in the summer of 2023 that shut down the city's computer networks for more than 2 weeks. Just 2 months ago Hayward began notifying individuals that personally identifiable information, including Social Security numbers and sensitive medical information had been breached as a part of the ransomware incident.

I know this story is not unusual and I'm sure my colleagues have also heard from local governments impacted by cyber attacks and looking for help. With cyber attacks coming from criminal gangs and nation-state adversaries we cannot leave our State and local governments to fend for themselves. Federal support for State and local governments is necessary to address the national security

threat and the State and Local Cybersecurity Grant Program has always reflected that understanding. By providing $1 billion to State, local, Tribal, and territorial governments Congress took a major step in strengthening our country's cyber defenses. For example, with a $250,000 grant from this program, a water utility can expand real-time monitoring to better detect and respond to cyber incidents, finally addressing a long-standing resourcing challenge in the water sector that we've heard about on this subcommittee for years.

When the State and Local Cybersecurity Grant Program was created, our primary concern was the ransomware epidemic that was plaguing our communities. That threat remains, but China's campaign to preposition on our critical infrastructure for potential future destructive attacks is even more alarming.

While much of our critical infrastructure is privately defended, some of our most vital services are provided by the public sector, publicly-owned and -operated water and electric utilities, transportation systems and emergency services could all be targets in destructive attacks by China or other adversaries. Reauthorizing the cybersecurity grant program is necessary to ensure we do not take our foot off the gas at this critical time in passing a reauthorization bill before this program expires in September is one of my top priorities on the committee.

What I've heard from stakeholders is an appreciation for the tremendous value of this program. We'll hear that today from our witnesses. But they also have a desire for sustained predictable and consistent funding levels that will allow State and governments to build on their progress and budget in plan their futures.

The program operates under a partnership between FEMA and CISA, 2 important agencies that unfortunately have come under attack in recent months. By leveraging FEMA's grants, administration expertise and CISA's cybersecurity expertise this program has been able to deliver for State and local governments in ways that would be impossible without that partnership.

Trump administration plans to eliminate FEMA and further cut CISA's work force would devastate Homeland Security's ability to support State and local governments across a range of threats, including cyber attacks. The Cybersecurity Grant Program demonstrates the value of collaboration between DHS's components and I hope we can work in a bipartisan way to further educate Secretary Noem about the tremendous value these agencies provide the American public.

I am also concerned about reports that FEMA has been pausing distributions of funding to implement cyber grants along with other programs. China is not pausing, they continue their efforts to target our critical infrastructure and we cannot pause either. The Trump administration must release cyber grant funds to States, territories, and Tribes to comply with court orders against any illegal process.

Again I want to thank the Chairman for holding this hearing, the witnesses for their participation, and look forward to expertise from both public and private sector, as we look to reauthorize this important program.

Thank you, Chairman. I yield back.

[The statement of Ranking Member Swalwell follows:]

STATEMENT OF RANKING MEMBER ERIC SWALWELL

APRIL 1, 2025

Establishing this program 4 years ago was the product of bipartisan legislation developed by this subcommittee, demonstrating how Members can come together to develop a solution that makes a meaningful difference in addressing a serious cybersecurity problem.

That kind of bipartisan work is just as necessary today, and I am confident today's hearing will help inform this subcommittee's efforts to extend necessary support to State and local governments.

As we consider State and local cyber grant reauthorization, it is important to remember that cyber attacks on State and local governments affect all our districts, whether they are in blue States or red States and whether they are urban, suburban, or rural.

In my district, the city of Hayward suffered a ransomware attack in the summer of 2023 that shut down the city's computer networks for more than 2 weeks.

And just 2 months ago, Hayward began notifying individuals that personally identifiable information, including social security numbers and sensitive medical information, had been breached as part of that ransomware incident.

I know this story is not unusual, and I am sure my colleagues have also heard from local governments impacted by cyber attacks and looking for help.

With cyber attacks coming from foreign criminal gangs and nation-state adversaries, we cannot leave our State and local governments to fend for themselves.

Federal support for State and local governments is necessary to address this national security threat, and the State and Local Cybersecurity Grant Program reflects that understanding.

By providing $1 billion to State, local, Tribal, and territorial governments, Congress took a major step in strengthening cyber defenses and bringing stakeholders together to develop and implement much-needed cybersecurity planning by State governments.

We are a more secure country today because of this investment.

But as we all know, our adversaries are not stopping their efforts to breach public-sector networks.

When the State and Local Cyber Grant Program was created, our primary concern was the ransomware epidemic plaguing our communities.

Of course, that threat remains, but China's campaign to pre-position on our critical infrastructure networks for potential future destructive attacks is even more alarming.

While much of our critical infrastructure is privately owned, some of our most vital services are provided by the public sector.

Publicly-owned and -operated water and electric utilities, transportation systems, and emergency services could all be targets in destructive attacks by China or other adversaries.

Reauthorizing the cybersecurity grant program is necessary to ensure we do not take our foot off the gas at this critical time, and passing a reauthorization bill before the program expires in September is one of my top priorities this year.

What I have heard from stakeholders is appreciation for the tremendous value of this program and a desire for sustained, predictable, and consistent funding levels that will allow State and local governments to build on their progress and properly budget and plan their efforts.

The cybersecurity grant program operates under a partnership between FEMA and CISA, two incredibly important agencies that have unfortunately come under attack in recent months.

By leveraging FEMA's grants administration expertise and CISA's cybersecurity expertise, this program has been able to deliver for State and local governments in ways that would be impossible without that partnership.

Trump administration plans to eliminate FEMA and further cut CISA's workforce would devastate DHS's ability to support State and local governments across a range of threats, including cyber attacks.

The cybersecurity grant program demonstrates the value of collaboration between DHS's components, and I hope we can work in a bipartisan way to better educate Secretary Noem about the tremendous value these agencies provide the American public.

Additionally, I am deeply concerned by reports that FEMA has been pausing distributions of funding to implement cyber grants, along with other grant programs.

China is not pausing their efforts to target our critical infrastructure. We should not pause our efforts to defend ourselves.

I urge the Trump administration to release cyber grant funds to States, territories, and Tribes and to comply with court orders against its illegal pauses.

Finally, I would like to thank the witnesses for appearing before us today.

Expertise from both the public and private sector is invaluable as we look to reauthorize and improve the State and Local Cybersecurity Grant Program, and I look forward to their testimony.

Mr. GARBARINO. The gentleman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

APRIL 1, 2025

Four years ago, bipartisan lawmakers led by Congresswoman Yvette Clarke and Chairman Garbarino passed legislation to establish a State and Local Cybersecurity Grant program.

I am pleased to have the opportunity to hear about the program's implementation today as we begin our important work on reauthorization.

When the State and Local Cybersecurity Grant program was initially enacted, the country was in the midst of a ransomware epidemic that cost local governments across the country millions of dollars—to say nothing of public services that couldn't be provided to taxpayers.

No part of the country was immune. Ransomware attacks hit cities from Atlanta to Albany, and a bipartisan consensus emerged that investing in prevention would not only ensure the continuity of public services but also save money in the long run.

By all accounts, the State and Local Cybersecurity Grant program is working.

According to stakeholders, the FEMA and CISA have been effective stewards of the program, soliciting and incorporating feedback from State and local governments to improve the program and make applications and drawdowns more efficient.

Incorporating lessons learned from previous grant programs, the Cybersecurity program required States to put in place governance structures and State Cybersecurity Plans to ensure Federal dollars were invested in a manner that would achieve the security goals set by Congress.

The relationships built through this process have facilitated new, strategic Statewide collaborations.

The most consistent piece of feedback I have received about the State and Local Cybersecurity Grant Program is that it must be reauthorized.

State and local governments have made significant progress hardening their information systems and building resilience, but there is more work to do.

And, unfortunately, cyber criminals continue to hold Government services hostage in hopes of cashing in.

Just under 2 years ago, a county in my district was hit by a ransomware attack, crippling information systems and disrupting basic services for the public like processing real estate transactions and providing car tags.

This one ransomware attack cost the county over half of a million dollars in recovery costs alone.

We also know that state actors are targeting publicly-owned critical infrastructure.

In late December 2023, Iranian hackers targeted small water utilities across the country.

And Volt Typhoon—a state-sponsored threat actor from China—has sought to gain access to critical infrastructure networks in order to execute destructive cyber attacks in the event of a U.S.-China conflict.

Congress would never leave State and local governments to fend for themselves in a physical attack. We cannot leave them to fend for themselves in cyber space.

Before I close, I would like to express my deep concern about recent actions the Trump administration has taken that frustrate the effectiveness of Federal grant programs.

I understand the President's grant freeze has interfered with the timely drawdown of grant funds. These delays create chaos for grantees and undermine the security goals of grant programs.

I also would like to express my opposition to the President's efforts to abolish FEMA and gut CISA.

These 2 agencies play central roles in the security and resilience of U.S. critical infrastructure, and we cannot afford to play fast and loose with them.

Finally, I want to be on the record objecting to CISA's cuts to the Multi-State Information and Analysis Center (MS–ISAC).

The MS–ISAC provides essential cybersecurity services to State and local governments. Fewer services means less security. And that's a price too high to pay.

Mr. GARBARINO. I am pleased to have a distinguished panel of witnesses before us today. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GARBARINO. Let the record reflect the witnesses answered in the affirmative. Thank you and please be seated.

I would now like to formally introduce our witnesses. Mr. Robert Huber, he currently serves as the chief security officer at Tenable. He oversees the organization's global security and research teams to reduce security risks to the company, its customers and industry. Prior to his private-sector career, Mr. Huber served in the U.S. Air Force and National Guard for 22 years.

Mr. Allen Fuller serves as the chief information officer for the State of Utah. In his role he oversees all IT functions for State executive branch agencies aiming to improve innovation and government services through technology. He also serves as the secretary of treasurer of the National Association of State Chief Information Officers.

The honorable Kevin Kramer is the first vice president of National League of Cities where he leads efforts of city, town, and village leaders to improve the quality of life for their residents. Additionally, Mr. Kramer serves as councilman for Louisville, Kentucky where he is the chair for the minority caucus, vice chair of the budget committee, and member of the government oversight audit appointments committee.

Mr. Mark Raymond is chief information officer for the State of Connecticut where he oversees the department of administrative services, bureau of information technology solutions, and holds operational responsibility for the State's technology infrastructure.

Prior to a public service career, Mr. Raymond spent 21 years in a technology consulting industry where he supported Federal, State, and local clients.

I thank the witness for being here today. I now recognize Mr. Huber for 5 minutes to summarize his opening statement.

STATEMENT OF ROBERT HUBER, CHIEF SECURITY OFFICER, TENABLE, INC.

Mr. HUBER. Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, thank you for the opportunity to testify today and for convening this important hearing. I'm Bob Huber, chief security officer, head of research and of public sector at Tenable, a cybersecurity exposure management company.

Tenable serves 44,000 customers worldwide, including the Federal Government as well as State, local, Tribal, and territorial governments and critical infrastructure operators. State and local governments play a crucial role in managing protecting critical infrastructure such as water treatment facilities, energy grids, transpor-

tation networks. They are on the front lines of defending these systems from cyber attacks that could disrupt vital services, erode public confidence, and compromise national security. Protecting essential systems is more urgent than ever. In 2023, the China-backed cyber espionage group Volt Typhoon, known for targeting critical infrastructure, attacked a Massachusetts utility. While disruptions were avoided, the incident showed the growing sophistication of adversaries who could position themselves to perpetrate future attacks on critical infrastructure.

In addition, ransomware attacks doubled between 2018 and 2024 causing over $1 billion in operational down time for State and local governments. These threats highlight the need for robust cybersecurity measures and coordinated efforts among all levels of government and the private sector detect, mitigate, and recover from these cyber threats.

The State and Local Cybersecurity Grant Program, or SLCGP, is a vital tool in addressing these challenges, providing $1 billion over 4 years to help State and local governments address cybersecurity risks.

To receive funds States have to follow a structured process, including establishing a cybersecurity planning committee to include State and local officials. Together they must develop a State border security plan that incorporates baseline requirements and alignment, cybersecurity best practices, and international standards.

States created different SLCGP programs. Some provided competitive grants while local governments could apply for funding for cybersecurity projects. Others provide shared services to local governments such as multifactor authentication, vulnerability management, or endpoint detection services. States like Connecticut, Utah, and Virginia are successful use cases of the SLCGP program. Virginia's whole-of-State approach focuses on collaboration, enterprise-level visibility, and efficient resource allocation. Virginia provided free cybersecurity planning capability assessments to local entities who could then apply for funding to address identified gaps through a streamlined application process. Eighty percent of eligible localities applied for the funding highlighting the need for assistance. Balanced central oversight with decentralized execution enabled Virginia to exercise its overall cybersecurity resilience.

SLCGP objectives include continuous monitoring, asset inventory and vulnerability prioritization, which are all essential components of the exposure management approach. Exposure management shifts organizations from a reactive approach to proactive. Risk-informed strategies across modern attack surfaces, such as operational technology iterative things, as well as cloud configurations. This proactive approach helps State and local agencies anticipate and mitigate risk before the impact vital systems.

SLCGP has significantly contributed to enhancing cybersecurity across State and local governments by providing essential funding, fostering collaboration, and encouraging strategic and proactive planning based on best practices. It has notably strengthened relationships between State and local officials through the cybersecurity planning committees and their collective development of the cybersecurity plans.

To continue and to build on SLCGP's success, Tenable recommends reauthorizing the program with the following improvements: ensure sustainable funding by extending the program's duration and enable long-term planning; maintaining alignment with recognized standards and frameworks such as the NIST cybersecurity framework; reducing the administrative burdens and providing clear guidance through simplified applications; and, lowering and leveling cost-share requirements for effective planning, continuing to encourage whole-of-State and proactive exposure management strategies and engaging the private sector and stakeholders to address evolving threats and best practices.

Continued success of the SLCGP program also depends on having qualified cybersecurity professionals at all levels to manage it. Tenable supports the enactment of the Cyber PIVOTT Act to address work-force shortages, to reach steelworkers and create diverse pathways into government cybersecurity careers.

Thank you again for your attention to cybersecurity, continued support of the SLCGP and for the opportunity to testify. I look forward to working with you to secure our Nation's cyber assets. I am happy to answer your questions. Thank you.

[The prepared statement of Mr. Huber follows:]

PREPARED STATEMENT OF ROBERT HUBER

APRIL 1, 2025

INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and Members of the subcommittee, thank you for the opportunity to testify before you today on the State and Local Cybersecurity Grant Program (SLCGP). I also commend the subcommittee for convening this important hearing and for your continued leadership in advancing cybersecurity and safeguarding our Nation's critical infrastructure. Your efforts are vital to strengthening the security and resilience of our communities, and I look forward to discussing how the SLCGP supports these priorities.

My name is Bob Huber and I am the chief security officer, head of research, and president of public sector at Tenable, a cybersecurity exposure management company that provides organizations, including Federal, State, and local governments, with an unmatched breadth of visibility and depth of analytics to measure and communicate cybersecurity risk. In collaboration with industry, Government, and academia, Tenable is raising awareness of the growing security risks impacting critical infrastructure and the need to take steps to mitigate those risks.

Prior to joining Tenable, I was a chief security and strategy officer at Eastwind Networks, and the co-founder and president of Critical Intelligence, an operational technology (OT) threat intelligence and solutions provider, which cyber threat intelligence leader iSIGHT Partners acquired in 2015. I served as a member of the Lockheed Martin Computer Incident Response Team (CIRT), an OT security researcher at Idaho National Laboratory, and was a chief security architect for JP Morgan Chase. I am a board member and advisor to several security start-ups and served in the U.S. Air Force and Air National Guard for more than 22 years. As a member of the Air National Guard, I provided support to the great State of Delaware for over 18 years, delivering security assessments of critical infrastructure throughout the State and CTAA (coordinate, train, advise, assist) in both title 32 and State active duty. Before retiring in 2021, I provided offensive and defensive cyber capabilities supporting the National Security Agency (NSA), United States Cyber Command, and State missions.

As Tenable's chief security officer, I oversee the company's global security and research teams, working cross-functionally to reduce risk to the organization, its customers, and the broader industry. This includes directing the Tenable Security Response Team in analyzing advanced threats like Volt Typhoon and Salt Typhoon, supporting vulnerability and asset management, leading the Tenable secure software development team, and promoting best practices such as Zero Trust and cyber

hygiene. I am also responsible for briefing Tenable's board of directors on our cybersecurity program and providing an overview of our key objectives and performance metrics.

My work to keep Tenable secure provides a similar vantage point as State and local government cybersecurity leaders when it comes to protecting an organization's assets and networks. Tenable adheres to several cybersecurity standards, frameworks and best practices to protect its own infrastructure and data. Tenable aligns its security program around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), and we are certified against the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001/27002 standard. Additionally, Tenable products are designed to support compliance with various security frameworks, including NIST CSF; ISO/IEC 27001/27002; and the Center for Internet Security (CIS) Critical Security Controls.

ABOUT TENABLE

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode organization value, reputation, and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight, and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe.

As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure nearly any digital asset on any computing platform, including operational technology (OT) and internet of things (IoT). Tenable customers include approximately 65 percent of the Fortune 500, approximately 50 percent of the Global 2000, and large Government agencies.[1] Approximately 15 percent of Tenable's business is related to the public sector. We collaborate with Federal agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) and advocate for strong baseline cybersecurity standards across critical infrastructure sectors. We are active in public-private partnerships with the Government through the President's National Security Telecommunications Advisory Committee (NSTAC), the IT Sector Coordinating Council (IT–SCC), the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC), and the NIST National Cyber Center of Excellence (NCCOE).

Tenable has been a long-standing strategic partner to State, local, Tribal, and territorial governments (SLTTs), providing a proactive risk-based approach to exposure management by helping them reduce risk with a unified view of all assets and resulting risk exposure.

THE THREAT LANDSCAPE FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS

State, local, Tribal, and territorial governments (SLTTs) play a significant role in safeguarding critical infrastructure, public services, and sensitive citizen data from an increasing array of cyber threats. They are at the forefront of cyber defense, overseeing public safety functions, regulating utilities, and managing essential systems such as water treatment facilities, transportation networks, energy grids, and communication systems. In addition to securing these critical operations, SLTTs are responsible for protecting vast amounts of personal data, including financial records and health information. Ensuring the security of these systems and data is essential not only for maintaining public trust, complying with privacy laws, and preventing costly disruptions, but also as a matter of national security. The stability and resilience of these systems are critical to the Nation's economic strength, defense capabilities, and overall safety, making SLTTs key players in the broader effort to protect the country from evolving cyber threats.

Advanced Persistent Threat Actors

This growing threat is exemplified by real-world cyber incidents that highlight the vulnerabilities of critical infrastructure and the potential consequences of such attacks. In 2023, Volt Typhoon, an advanced persistent threat (APT) actor backed by the People's Republic of China (PRC), launched a prolonged cyber attack on the Littleton Electric Light and Water Departments (LELWD) in Massachusetts, the

[1] Tenable, "About Tenable," *www.tenable.com.*

first known strike on a U.S. power utility by the group.[2] The attack targeted the utility's operational technology (OT) infrastructure in an effort to exfiltrate sensitive data. Although LELWD was able to detect and mitigate the breach before major disruptions occurred, the incident underscored the increasing sophistication of nation-state cyber threats and the risks they pose to essential services.

This attack was not an isolated incident but part of a broader pattern of cyber espionage and disruption orchestrated by Volt Typhoon. Government officials, including former National Security Agency (NSA) Cybersecurity Director Rob Joyce, have expressed growing concerns about the escalating threat posed by China-backed hacking campaigns, including Volt Typhoon. These threat actors have latched onto critical infrastructure through compromised equipment including internet routers and cameras. According to Joyce, the NSA continues its efforts to eradicate such threats and the United States is still finding victims of the Volt Typhoon hacking collective.[3] It is encouraging to see Members of this committee, including Chairman Mark Green, Chairman Andrew Garbarino, and Congressman Josh Brecheen prioritize investigations into these Chinese-backed intrusions, calling on the Department of Homeland Security (DHS) to assess the Federal Government's response and strengthen the resilience of America's cybersecurity posture.[4]

The increase in activity from APT actors targeting U.S. critical infrastructure,[5] as highlighted in the Office of the Director of National Intelligence (ODNI) 2025 Annual Threat Assessment of the U.S. intelligence community, reinforces the need for heightened vigilance at the State and local levels.[6] The PRC remains the most active and persistent threat to U.S. critical infrastructure, much of which is managed by both public and private-sector entities. Safeguarding against such sophisticated threats demands coordinated efforts between national intelligence agencies, Federal civilian agencies, and State and local governments. Only through this coordinated approach can the United States effectively detect, mitigate, and recover from these cyber attacks, securing the Nation's critical systems and protecting national security.

Ransomware

In addition to these significant threats, States also face the growing prevalence of ransomware attacks. From 2018 to 2024, incidents of ransomware attacks targeting State and local government organizations have doubled. A recent study by Comparitech found that over 500 ransomware attacks were carried out during that time, resulting in more than $1 billion in operational downtime.[7]

The Center for Internet Security's (CIS) 2023 National Cybersecurity Review similarly revealed a sharp rise in cyber attacks targeting State and local government organizations during the first 8 months of 2023 compared to the same period in 2022.[8] Malware attacks surged by 148 percent and CIS's Review also found ransomware incidents on the rise, climbing by 51 percent during this time period. Non-malware attacks grew by 37 percent, encompassing activities like command shell usage and suspicious Secure Sockets Layer (SSL) certificate detections.[9]

Another concerning trend highlighted in the study was a startling 313 percent rise in endpoint security service incidents, suggesting a significant uptick in breaches and unauthorized access attempts.[10] These findings further underline the

---

[2] Waqas, "Chinese Volt Typhoon Hackers Infiltrated US Electric Utility for Nearly a Year," Hack Read, March 12, 2025, *https://hackread.com/chinese-volt-typhoon-hackers-infiltrated-us-electric-grid.*

[3] David DiMolfetta, "U.S. still finding victims of advanced China-linked hacking campaign, NSA official says," Nextgov/FCW, March 14, 2025, *https://www.nextgov.com/cybersecurity/2024/03/us-still-finding-victims-advanced-china-linked-hacking-campaign-nsa-official-says.*

[4] Chairman Mark Green, Chairman Andrew Garbarino, and Congressman Josh Brecheen, *Congressional Letter to the Department of Homeland Security (DHS) Secretary Kristi Noem on Volt Typhoon and Salt Typhoon,* March 17, 2025, *2025-03-17-Green-Garbarino-Brecheen-to-Noem-DHS-re-Volt-and-Salt-Typhoon.pdf.*

[5] CISA, *PRC State-Sponsored Actors Compromise and Persistent Access to U.S. Critical Infrastructure,* Feb. 7, 2024, *https://www.cisa.gov/news-events/cybersecurity-advisories*.

[6] ODNI, *2025 Annual Threat Assessment of the U.S. Intelligence Community,* March 2025, *ATA–2025-Unclassified-Report.pdf.*

[7] Comparitech, *Ransomware attacks on US government organizations have cost over $1.09 billion,* March 18, 2025, *https://www.comparitech.com/blog/information-security/government-ransomware-attacks.*

[8] Center for Internet Security, *Nationwide Cybersecurity Review: 2023 Summary Report,* Sept. 27, 2024, *https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report.*

[9] 8. Ibid.

[10] 9. Ibid.

escalating threat landscape for State and local governments, emphasizing the urgent need for improved cybersecurity measures to protect sensitive systems and data from these increasingly complex and persistent attacks.

RISK MANAGEMENT EXECUTIVE ORDER

In an effort to empower State, local, and individual efforts in enhancing national resilience and preparedness, the current administration released Executive Order (EO) 14239: Achieving Efficiency Through State and Local Preparedness, which aims to create more resilient infrastructure and address risks, including cyber attacks.[11] Specifically, the EO "calls for a review of all infrastructure, continuity, and preparedness policies to modernize and simplify Federal approaches, aligning them with the National Resilience Strategy."[12]

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

Given the on-going threats and increasing responsibilities of State and local governments in managing cybersecurity risks, the State and Local Cybersecurity Grant Program (SLCGP) is more important than ever. Administered by the Cybersecurity and Infrastructure Security Agency (CISA) in collaboration with the Federal Emergency Management Agency (FEMA), SLCGP provides $1 billion over 4 years to help State, local, Tribal, and territorial governments (SLTTs) enhance their cybersecurity capabilities and protect critical infrastructure from evolving threats.

To receive SLCGP funding, States follow a structured process, beginning with the establishment of a Cybersecurity Planning Committee. The committee must include representatives from various sectors, such as State CIOs, CISOs, election infrastructure, public safety, emergency management, and law enforcement. The committee is responsible for developing and revising the State's Cybersecurity Plan, which must incorporate baseline cybersecurity requirements that meet cybersecurity best practices and recognized standards identified in the SLCGP legislation, ensure the Plan reflects the input of local governments, outline responsibilities for State and local entities, include metrics to measure progress, and summarize associated projects. Additionally, States must conduct capability assessments to evaluate their current cybersecurity posture and meet Federal cost-share requirements.

By reducing financial barriers, SLCGP enables State and local governments to implement essential protections that safeguard their networks and critical infrastructure. Reauthorization of the program is vital to ensure that State and local governments have the resources they need to safeguard the Nation's critical infrastructure.

Examples of State SLCGP Programs

States have customized their SLCGP funding strategies to align with their unique governance structures and local government needs. Some examples include:

Collaborative Whole-of-State Approach.—Virginia serves as a great example of a whole-of-State approach for SLCGP, which provides enterprise-level visibility, valuable lessons learned, and strong collaboration among the participants. In Phase 1, Virginia offered a "Cybersecurity Plan Capability Assessment" at no cost to local entities. This assessment provided baseline cybersecurity evaluations and recommendations to address identified gaps in alignment with Virginia's Cybersecurity Plan, such as intrusion detection and response, vulnerability management, enhancing data recovery capabilities, and improving cybersecurity maturity levels.

Following the assessment, local entities could apply for Phase 2 funding to get the technology needed to increase their cybersecurity maturity. Virginia designed the application process to be straightforward and accessible, minimizing administrative burdens, particularly for smaller and rural jurisdictions. To support applicants, the State offers technical assistance and hosts information sessions to guide them through the process. As a result, 80 percent of eligible localities State-wide had at least one application for cybersecurity improvements, so demand for this type of assistance is high given the increased risk of cyber threats due to localities having fewer resources and funding opportunities.

By balancing centralized oversight with decentralized execution—and leveraging shared capabilities, strategic planning, and common technology—Virginia ensures that localities effectively utilize the funding while maintaining alignment with its Cybersecurity Plan and State-wide cybersecurity objectives. This whole-of-State strategy strengthens cybersecurity resilience across all levels of government.

---

[11] The White House, *Achieving Efficiency Through State and Local Preparedness,* March 19, 2025, *https://www.whitehouse.gov/presidential-actions/2025/03/test/*.

[12] 11. Ibid.

Competitive Grants Model.—Some States are focused on providing competitive grants for local government agencies and eligible entities. Applicants apply for funding for cybersecurity projects that align with SLCGP program requirements and the State's Cybersecurity Plan.

Hybrid Model with Competitive Grants and Shared Services.—Other States are adopting a hybrid model, blending competitive grant opportunities with direct in-kind services for local and Tribal governments. Local entities can apply for funding to support cybersecurity initiatives. Simultaneously, the State serves as a cybersecurity service provider, offering direct support to localities that may lack the resources to implement these initiatives independently. This strategy ensures that resources are distributed equitably while fostering alignment between local implementation and State-wide cybersecurity priorities, creating a more resilient and collaborative cybersecurity environment.

STATE APPROACHES TO CYBERSECURITY

The cybersecurity of State systems and infrastructure varies widely due to differences in resources, governance structures, and strategic approaches. Some States have adopted a "whole-of-State" approach, unifying State and local entities under a single cybersecurity framework, often with shared service programs for local governments. Others operate under a decentralized model, where individual State agencies or local governments manage their own cybersecurity infrastructure and policies independently, without centralized coordination.

Many States are establishing fusion centers that serve as hubs for gathering, analyzing, and sharing threat intelligence among Federal, State, local, Tribal, and private-sector partners. These centers often facilitate collaboration between law enforcement and IT professionals. Additionally, some States are creating regional security operations centers (RSOCs) to provide centralized monitoring and incident response capabilities, helping smaller jurisdictions with limited resources access advanced threat detection tools.

States are also leveraging Federal support, such as the Department of Homeland Security's bulk purchasing agreements, which lower costs for cybersecurity solutions. CISA offers free services, including vulnerability scanning, penetration testing, and malicious domain blocking, to help State and local governments mitigate cyber threats. Despite these efforts, many States face common challenges, including limited funding, a shortage of skilled personnel, and the absence of a cohesive, State-wide understanding of cyber risk.

BENEFITS OF EXPOSURE MANAGEMENT

As States adopt new technologies, they are often accompanied by new threats. In response, many security teams simply add a new siloed security tool and team to defend that new attack surface. As a result, security has become disjointed. The end result is fragmented visibility with gaps that leave State and local agencies vulnerable. Exposure management addresses this challenge by providing a more comprehensive understanding of risk.

Exposure management, which is aligned with the NIST Cybersecurity Framework, supports a more cost-effective and strategic approach to cybersecurity, continuously assessing the accessibility, exploitability, and criticality of all digital assets. By implementing an exposure management strategy, State and local governments will be better-equipped to secure their expanded environment, including critical infrastructure, in the face of increasing cyber threats and campaigns from nation-state attackers. This proactive, risk-informed approach aligns with the Executive Order on "Achieving Efficiency Through State and Local Preparedness," allowing State and local governments to take a proactive, risk-informed approach that prioritizes cybersecurity efforts based on actual threats, toxic risk combinations and attack path analysis, optimizing resource allocation and improving security resilience.

Unlike traditional cybersecurity strategies that focus solely on vulnerabilities, exposure management takes a broader view across the modern attack surface to provide a more comprehensive understanding of risk. It incorporates both technical and contextual factors such as vulnerabilities, misconfigurations, and attack paths—leveraging data from a spectrum of assets and technologies, including OT environments and IoT devices, cloud configurations, identity solutions, and web applications. This enables State and local agencies to prioritize issues that pose the most risk from across their infrastructure, making it easier to mitigate risks before they impact critical systems.

By implementing exposure management, State and local governments can shift from reactive to proactive security, prioritizing risks based on immediate threat in-

telligence and the attacker's perspective. This approach aligns with the Executive Order's efficiency goals, strengthening cybersecurity posture and enhancing preparedness to prevent attacks on critical infrastructure.

As State and local governments take on a more active role in cyber attack preparedness, it is critical to incorporate OT and IoT protection into an Exposure Management strategy. Most attacks on critical infrastructure originate in IT networks and 90 percent of attackers' initial access was gained via identity compromises.[13] In converged environments, it is critical to include IT assets in discovery processes because they often interact with OT systems and can serve as entry points for attackers to then move laterally to disrupt physical processes and operations. Ensuring SLTTs have a holistic view of their attack surface—from IT to OT and everywhere in between—helps them to understand exposure, close attack paths, and reduce risk. Strengthening the cybersecurity of these systems not only protects essential services but also increases resilience with the ability to anticipate, withstand, and quickly recover from cyber attacks.

BENEFITS OF WHOLE-OF-STATE APPROACH TO CYBERSECURITY

A whole-of-State approach fosters State-wide collaboration, strengthening the cybersecurity posture of all stakeholders while creating a unified and resilient defense strategy. By integrating the complex ecosystem of networks and systems under a standardized framework of policies, procedures, and controls, this approach enables State governments to optimize resources and extend cybersecurity support to local governments, educational institutions, and other organizations. The sharing of resources enhances the security of both State and local entities, reducing redundancies and improving overall efficiency. A unified approach streamlines processes, accelerates incident response, and facilitates reporting and compliance, ensuring a more proactive and coordinated cybersecurity strategy to reduce State-wide risk. Whole-of-State cybersecurity recognizes that SLTTs have a wide range of interconnected assets and systems. An attack on one part of the system can affect any or all of the others, compromising the security of the entire State, and for this reason, a coordinated and collaborative effort is recommended to secure the entire system.

WHAT'S WORKING WITH SLCGP

The State and Local Cybersecurity Grant Program (SLCGP) has laid a strong foundation for improving the cybersecurity posture of State and local governments by fostering collaboration, enhancing cybersecurity strategic planning, funding priority projects, and increasing visibility into local government cybersecurity needs.

Funding.—The funding provided by SLCGP is vital for SLTTs because many of these entities lack sufficient resources to address the growing complexity and scale of cyber threats. SLTTs often operate on limited budgets, and prioritize essential services like public safety, education, and infrastructure maintenance, leaving cybersecurity underfunded despite its critical importance. SLCGP funding helps bridge this gap by providing financial support for activities such as risk assessments, workforce training, governance planning, and the implementation of cybersecurity tools. It also enables smaller jurisdictions to access resources they might otherwise be unable to afford. By addressing systemic cyber risks through these targeted investments, SLCGP ensures that SLTTs can better protect their networks, critical infrastructure, and constituents from evolving cyber threats.

Relationship Building and Collaboration.—A key benefit of SLCGP is the strengthened relationships between State and local officials. The program mandates the creation of Cybersecurity Planning Committees, which must include representatives from various jurisdictions—urban, suburban, and rural—alongside State officials, and it requires local governments to have meaningful input into the State's Cybersecurity Plan. This inclusive governance structure encourages collaboration and open communication, and fosters trust and alignment between State and local officials in addressing shared risks.

Development of Cybersecurity Plans Aligned with Standards and Best Practices.—Another advantage of SLCGP is its requirement for States to develop Cybersecurity Plans. These Plans must incorporate elements that align with recognized cybersecurity standards and best practices to ensure a comprehensive and effective approach to improving cybersecurity State-wide. These requirements promote addressing risks proactively while providing a clear road map for enhancing resilience against cybersecurity threats.

---

[13] CISA, *CISA Analysis Fiscal Year 2022 Risk and Vulnerability Assessments,* June 2023, *https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final__508c.pdf.*

Visibility into Local Government Cybersecurity Needs.—SLCGP enhances visibility into local government cybersecurity needs by requiring States to engage with local entities during the planning process. Through assessments and feedback mechanisms, States gain a deeper understanding of the unique challenges faced by municipalities and rural areas. This enhanced visibility enables the development of tailored solutions that address specific vulnerabilities while aligning with broader State-wide priorities. By bridging the gap between State-level oversight and local implementation, the program ensures a coordinated and cohesive approach to strengthening cybersecurity infrastructure.

Encourages a whole-of-State approach to cybersecurity.—SLCGP's governance requirements—such as the creation of Cybersecurity Planning Committees and Cybersecurity Plans that involve State and local government officials and other stakeholders—promotes a whole-of-State approach to cybersecurity. As mentioned above, this approach fosters collaboration across the State, strengthens the cybersecurity posture of all parties, enables the sharing of resources, allows for economies of scale, reduces redundancies, improves overall efficiency, and creates a unified and resilient defense strategy.

POLICY RECOMMENDATIONS

Reauthorization of State and Local Cybersecurity Grant Program.—SLCGP has established a strong foundation for State and local governments to improve their cybersecurity posture. Tenable strongly encourages Congress to reauthorize SLCGP to ensure SLTTs continue to have the necessary resources and support required to address the increasingly sophisticated threats and increased responsibilities to protect their systems and critical infrastructure. Tenable also recommends the following improvements to the program:

- *Sustainable and Predictable Funding*.—Cyber threats are growing increasingly sophisticated, and critical infrastructure sectors such as water utilities and public services remain vulnerable. Sustained Federal investment is essential to ensure these entities can continue building resilient systems capable of defending against evolving risks. In addition, most cybersecurity programs require at least 18 months to implement and see positive effects. More predictable funding is essential for building sustainable cybersecurity capabilities. The current 4-year cycle creates uncertainty, discouraging States from investing in multi-year projects or infrastructure that may lose funding after 2026. Extending the program's duration would provide States with the confidence to plan long-term initiatives, maintain momentum, and develop lasting cybersecurity protections.
- *Alignment with Established Cybersecurity Standards and Best Practices*.—State Cybersecurity Plans and projects should continue to align with established cybersecurity best practices and standards, such as the NIST Cybersecurity Framework, CIS Critical Security Controls, and other recognized guidelines. Adopting these standards ensures that State and local governments leverage proven methodologies, rather than reinventing processes, saving time and resources while addressing systemic risks. In addition, we strongly encourage SLCGP to incorporate assessments against NIST's Cybersecurity Framework to identify the most significant risks, prioritize them, and provide a detailed roadmap for execution.
- *Simplifying Grant Application Process*.—A streamlined application process for States, clear guidance for grant application requirements, concise instructions, and clear expectations would help States navigate the process more effectively and reduce administrative burden.
- *Consistent Cost-Sharing Requirements*.—The increase in cost-share requirements—rising from 10 percent in fiscal year 2022 to 40 percent by fiscal year 2025—pose significant challenges for States and local governments, particularly rural areas with limited budgets. This escalating financial burden can strain State budgets, especially since many are planned years in advance and may not accommodate these rising costs.[14] Additionally, smaller and rural jurisdictions often struggle to meet the match requirements, even with creative solutions like in-kind contributions. Establishing a lower and consistent match percentage would reduce financial strain, promote equitable access to funding, and enable States to conduct long-term cybersecurity planning.
- *Risk Management Approach*.—Encourage the adoption of exposure management, which helps States and local governments assess and mitigate risks to critical infrastructure. Exposure management strategies enable a proactive,

[14] FEMA, *State and Local Cybersecurity Grant Program, https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program.*

risk-informed approach, improving resource allocation and security resilience against evolving threats.

- *Active Stakeholder Engagement*.—Active stakeholder engagement is critical in both the development and implementation of the SLCGP program. CISA can leverage private-sector stakeholder expertise to ensure the program adapts as the threat landscape evolves. States and localities can learn from practitioners what processes and practices are demonstrating effectiveness in mitigating risks and countering threat activity.

  By addressing these issues, a reauthorized SLCGP could better equip State and local governments to manage systemic cyber risks while fostering sustainability, accessibility, and resilience in their cybersecurity infrastructure.
- *Workforce Development*.—Tenable strongly encourages Congress to enact the Cyber PIVOTT Act to help close the national cybersecurity workforce gap by creating a talent pipeline for government service. Modeled after the ROTC framework, the Cyber PIVOTT Act offers full scholarships for 2-year degrees at community colleges and technical schools in exchange for government service at the Federal, State, or local level.[15] This initiative not only reskills and upskills workers but also provides a pathway for individuals from different backgrounds to "pivot" into cybersecurity careers. By integrating such programs into SLCGP-funded workforce development strategies, States can build a sustainable and skilled cybersecurity workforce capable of protecting critical infrastructure and addressing emerging cyber threats. Additionally, expanding training programs for government personnel at all levels should be prioritized to ensure that employees are equipped to manage evolving threats.

CONCLUSION

Tenable recommends several key actions for Congress to strengthen the cybersecurity capabilities of State, local, Tribal, and territorial governments, including reauthorizing and improving the State and Local Cybersecurity Grant Program and prioritizing workforce development through initiatives like the Cyber PIVOTT Act. These steps will help enhance State, local, Tribal, and territorial governments' ability to protect critical infrastructure.

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson, and Members of the subcommittee, thank you for the opportunity to testify before you today on the importance of the State and Local Cybersecurity Grant Program. I appreciate the committee's continued bipartisan work to address the growing cybersecurity challenges our Nation faces. As the threat landscape evolves, it is crucial that State, local, Tribal, and territorial governments have the support to improve their cybersecurity defenses. I look forward to collaborating with you all to ensure we provide the necessary funding and resources to protect our communities and critical infrastructure.

Mr. GARBARINO. Thank you, Mr. Huber.

I now recognize Mr. Fuller for 5 minutes to summarize his opening statement.

STATEMENT OF ALAN FULLER, CHIEF INFORMATION OFFICER, STATE OF UTAH

Mr. FULLER. Thank you, Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee. It is a pleasure to be with you today. I'm Allen Fuller, chief information officer for the State of Utah, a role to which I was appointed by Governor Cox in March 2021. As the CIO for the State I lead the division of technology services, which is the consolidated IT organization for all of the executive branch agencies at the State. As part of my team, I oversee the cyber center, which is responsible for defending State IT assistance against cyber crime.

I'm also secretary-treasurer for the National Association of State Chief Information Officers or NASCIO. NASCIO is a national lead-

[15] Chairman Mark Green, *Press Release: Chairman Green Reintroduces "Cyber PIVOTT Act," Senator Rounds to Lead Companion Legislation,* Feb. 5, 2025, *https://homeland.house.gov/2025/02/05/chairman-green-reintroduces-cyber-pivott-act-senator-rounds-to-lead-companion-legislation/*.

er and advocate for technology policy at all levels of government and has championed substantial collaboration between States and the Federal Government to improve cybersecurity preparedness and protect or Nation's critical infrastructure. So as both CIO to the State of Utah and as a NASCIO officer, I hope to highlight the may successes of the State and local cybersecurity program or SLCGP today.

This program was provided significant—support the States in and local governments as we have worked together to improve cybersecurity posture and to address vulnerabilities. Over the past decade in Utah, State, county, city governments witness significant escalations and cyber incidents. Initially attacks were less frequent and less sophisticated, often targeting basic vulnerabilities. However, recent years have seen a surge in complex ransomware attacks, data breaches, and phishing campaigns, specifically designed to exploit government systems. This evolution reflects a broader trend where malicious actors increasingly target public-sector entities seeking to disrupt services, extort funds, and compromise sensitive data.

Local governments in particular face challenges in keeping pace with these threats due to budget constraints and limited cybersecurity expertise, making them more susceptible to these evolving cyber risks.

In Utah we applied for SLCGP funds in 2022 and received approximately $13 million of Federal funds and $4 million in matching State funds for local cybersecurity efforts. Assessments and audits were conducted to identify the strength that cybersecurity defenses around the State, including cities, counties, and higher education entities results found the cybersecurity systems were significantly under-developed in many cases, leaving local government entities at serious risks.

Note that many of these cities and counties have limited resources with very little or no IT support. The SLCGP is being utilized to address those concerns by providing much-needed tools to local entities. With funding secure through the SLCGP and course-aligned State appropriations, a comprehensive cybersecurity initiative has been deployed across 140 governmental entities in the State. These include 23 counties, 94 municipalities, and 23 special districts. Through this effort endpoint security has been the provision for over 26,000 devices. And cybersecurity awareness training is being delivered to 31,000 local government employees. The program includes scheduled engagements with local leaders to guide the progression of State-wide cybersecurity initiatives. The results have been extremely positive. We have blocked 7 major cyber-attack incidents in the last 6 months alone.

I will speak to 2 of these. Shortly before Christmas the CIO of the local airport urgently contacted me about a cyber attack in progress. The cyber criminals attempted to deploy ransomware on the airport's IT systems, which would have been disastrous, especially during the busy holiday travel season. Our cyber center team immediately worked with the airport's IT team to address the issue. Fortunately, SLCGP funds have provided security tools, are able to detect and interrupt the attack as it was happening. The common tooling and established relationships with local staff en-

abled a rapid response and limited the impact of the attack. As a result, the airport service was not interrupted and no ransom was paid.

Second, recently a 9–1–1 emergency dispatch center in Utah was a victim of ransomware attack on systems that provide 9–1–1 services. Again, SLCGP funds have provided security tools that detected and interrupted the attack as it was happening. Common tooling and established relationships enabled a rapid response that limited the attack's impact. Critical 9–1–1 dispatch services were able to continue in one of our biggest counties.

Utah's positive experience to this grant program is not an outlier. SLCGP has allowed many States to embrace a whole-of-State approach to cybersecurity. By approaching cybersecurity jointly, information is widely shared, and incident response is more effective. States have been able to use SLCGP to provide a vital technology of services and many smaller communities simply would not be able to implement.

The State and Local Cybersecurity Grant Program helps stakeholders developing a solid foundation on which to continue to strengthen their defenses and to modernize both their technology and their processes. I encourage the subcommittee to extend funding for the program.

I look forward to discussing it today and to answering your questions. Thank you very much.

[The prepared statement of Mr. Fuller follows:]

PREPARED STATEMENT OF ALAN FULLER

APRIL 1, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee: I am Alan Fuller, chief information officer for the State of Utah, a role to which I was appointed by Governor Cox in March 2021. As CIO for the State of Utah, I lead the Division of Technology Services, the consolidated IT organization for the executive branch agencies in the State government. As part of my team, I oversee the Cyber Center, which is responsible for defending State IT systems against cyber crime. The Utah Cyber Center *(cybercenter.utah.gov)* was created to coordinate efforts between State, local, and Federal resources to bolster State-wide security and help defend against future cyber attacks, by sharing cyber threat intelligence, best practices, and through strategic partnerships.

I am also the secretary-treasurer for the National Association of Chief Information Officers (NASCIO.) NASCIO is the collective voice of the Nation's State and territorial chief information officers, chief information security officers, and chief privacy officers. Its mission is to advance government excellence through trusted collaboration, partnerships, and technology leadership. NASCIO is a national leader and advocate for technology policy at all levels of government, and has championed substantial collaboration between States and the Federal Government to improve cybersecurity preparedness and protect our Nation's critical infrastructure.

It is as both CIO for the State of Utah and as a NASCIO officer that I hope to highlight the many successes of the State and Local Cybersecurity Grant Program (SLCGP) today. Though no program is perfect, SLCGP has provided significant support to States and local governments as we have worked to improve our cybersecurity posture and address vulnerabilities.

UTAH'S EXPERIENCE

Over the past decade in Utah, State, county, and city governments have witnessed significant escalations in cyber incidents. Initially, attacks were less frequent and sophisticated, often targeting basic vulnerabilities. However, recent years have seen a surge in complex ransomware attacks, data breaches, and phishing campaigns specifically designed to exploit government systems. This evolution reflects a broader trend where malicious actors increasingly target public-sector entities, seeking to

disrupt services, extort funds, and compromise sensitive data. Local governments, in particular, face challenges in keeping pace with these threats due to budget constraints and limited cybersecurity expertise, making them more susceptible to these evolving cyber risks. Before implementation of the SLCGP, incidents were not reported to the State for fear the State's role would be punitive in nature. If the State was notified, options for response were very limited as either data had already been compromised or system damage, such as ransomware, had already been executed. In many instances, paying a ransom or providing credit monitoring for victims were the only recovery options.

In Utah, we applied for SLCGP funds in 2022 and received approximately $13 million Federal funds and $4 million in matching State funds for local cybersecurity efforts. Assessments and audits were conducted to identify any existing cybersecurity issues around the State, including cities, counties, local education agencies, and higher education entities. Results found that cybersecurity systems are significantly under-developed in many cases, leaving local government entities with serious risks (Image 1).

Image 1: Assessment of Cybersecurity Risk for Utah Local Entities

Relative NIST Maturity Level

Low — High

Level in Hierarchy	Control Abbreviation	Control Description	Central Security Services	Entity A	Entity B	Entity C	Entity D	Entity E	Entity F	Entity G	Entity H	Entity I	Entity J	Entity K	Entity L	Entity M	Entity N	Entity O	Entity P	Entity Q	Entity R	Average
Overall			3.62	2.4	2.3	1.6	1.9	2.4	1.3	1.4	1.6	2.2	2.3	2.9	2.4	1.5	1.6	2.0	1.7	2.5	2.4	2.1
Function	ID	IDENTIFY	3.69	2.5	2.0	1.8	2.2	2.7	1.4	1.4	1.3	1.8	2.5	2.9	2.4	1.6	2.1	2.1	1.7	2.3	2.8	2.1
	PR	PROTECT	3.82	3.0	2.3	2.0	2.3	2.8	1.6	1.8	1.9	2.1	2.6	3.1	2.6	1.8	1.9	2.2	1.9	2.6	2.8	2.3
	DE	DETECT	3.60	2.3	3.0	1.6	2.1	2.2	1.3	1.7	2.0	3.0	1.9	3.3	2.5	1.5	1.4	2.0	1.4	2.0	1.9	2.1
	RS	RESPOND	4.38	2.2	2.7	1.4	2.0	2.3	1.1	1.3	1.7	2.8	2.4	3.0	2.4	1.6	1.4	2.2	1.7	2.3	2.0	2.0
	RC	RECOVER	2.83	1.9	1.7	1.3	1.1	1.9	1.1	1.0	1.0	1.2	2.1	2.0	2.1	1.7	1.7	1.7	1.6	1.7	2.5	1.7
Category	ID.AM	Asset Management	4.19	3.1	2.1	1.9	2.9	3.4	1.9	1.7	2.0	2.4	3.0	3.2	2.5	1.5	2.3	2.1	2.0	3.0	3.0	2.5
	ID.BE	Business Environment	3.92	2.4	1.9	1.6	1.9	2.5	1.3	1.2	1.1	1.7	2.7	2.5	2.3	1.5	2.3	2.2	1.5	2.4	3.0	2.0
	ID.GV	Governance	4.20	2.5	2.0	1.7	2.3	2.7	1.4	1.4	1.1	2.0	2.7	3.4	2.3	1.4	2.6	2.4	1.7	2.5	2.8	2.2
	ID.RA	Risk Assessment	3.68	2.6	2.3	1.7	2.3	2.6	1.2	1.7	1.5	2.2	2.3	3.5	2.3	1.7	2.0	2.0	1.6	2.0	2.5	2.1
	ID.RM	Risk Management Strategy	3.77	2.1	1.6	2.0	2.2	2.6	1.2	1.1	1.1	1.2	2.2	3.0	2.4	2.1	2.4	2.1	1.7	2.0	3.1	2.0
	ID.SC	Supply Chain Risk Management	2.37	2.0	1.9	1.8	1.6	2.4	1.1	1.1	1.1	1.1	2.1	1.8	2.8	1.3	1.3	1.8	1.5	2.1	2.4	1.7
	PR.AC	Identity Management, Authentication and Access Control	4.49	3.6	2.6	2.5	2.9	3.0	1.9	2.1	2.5	2.8	2.5	3.3	2.9	2.3	2.2	2.4	2.3	2.8	2.9	2.6
	PR.AT	Awareness and Training	3.68	2.5	3.0	2.2	1.8	3.0	1.3	1.8	1.2	1.5	2.9	3.7	3.2	1.7	1.3	2.3	1.6	3.0	3.3	2.3
	PR.DS	Data Security	3.74	2.8	3.5	1.7	1.7	2.5	1.4	1.7	2.1	1.6	2.4	2.4	2.4	1.5	1.6	1.8	2.0	2.1	2.3	2.0
	PR.IP	Information Protection Processes and Procedures	3.61	2.8	2.2	1.8	2.0	2.6	1.6	1.6	1.7	2.2	2.3	3.2	2.4	1.7	2.1	2.1	2.0	2.5	2.8	2.2
	PR.MA	Maintenance	3.52	3.3	2.3	2.2	3.0	2.9	1.7	2.3	1.8	2.1	3.2	3.3	2.6	2.1	2.0	2.3	2.0	3.1	3.4	2.5
	PR.PT	Protective Technology	3.89	3.2	2.9	1.8	2.4	2.9	1.4	1.5	2.1	2.4	2.5	2.9	2.4	1.7	1.7	2.1	1.7	2.4	2.3	2.2
	DE.AE	Anomalies and Events	3.94	2.2	3.2	1.5	1.9	2.3	1.3	1.7	2.0	3.3	2.2	3.3	2.5	1.3	1.4	2.2	1.4	1.9	1.8	2.1
	DE.CM	Security Continuous Monitoring	3.44	2.7	2.9	1.9	2.2	2.5	1.4	2.1	2.4	2.9	1.7	3.4	2.8	1.8	1.5	2.3	1.6	2.3	2.2	2.2
	DE.DP	Detection Processes	3.43	2.3	2.9	1.5	2.2	1.8	1.2	1.4	1.5	2.8	1.8	3.1	2.3	1.3	1.5	1.7	1.4	1.8	1.6	1.9
	RS.RP	Response Planning	4.92	2.0	2.7	1.2	2.1	2.2	1.0	1.2	2.1	3.0	2.6	2.6	2.5	1.6	1.3	2.3	1.8	2.3	1.8	2.0
	RS.CO	Communications	4.14	2.5	2.9	1.7	1.9	2.6	1.3	1.3	1.7	2.8	2.4	3.2	2.4	1.6	1.6	2.2	1.5	2.4	2.1	2.1
	RS.AN	Analysis	3.70	2.1	2.9	1.5	1.7	2.3	1.1	1.4	1.6	2.9	2.3	3.2	2.2	1.4	1.4	2.2	1.6	2.1	2.0	2.0
	RS.MI	Mitigation	3.81	2.1	2.5	1.5	1.9	2.4	1.0	1.2	1.6	2.3	2.4	3.0	2.3	1.8	1.5	2.2	1.5	1.9	2.1	2.0
	RS.IM	Improvements	4.33	2.3	2.6	1.1	2.3	1.8	1.0	1.1	1.6	2.8	2.4	3.2	2.6	1.4	1.1	2.0	1.9	2.9	2.2	2.0
	RC.RP	Recovery Planning	3.00	2.3	1.7	1.0	1.0	1.7	1.0	1.0	1.0	1.0	2.7	2.3	2.0	1.0	1.0	1.7	1.3	3.7	3.0	1.7
	RC.IM	Improvements	2.43	1.6	1.1	1.1	1.0	1.9	1.0	1.0	1.0	1.0	1.6	1.6	2.3	1.1	1.0	1.4	1.5	3.1	2.5	1.5
	RC.CO	Communications	3.07	1.7	2.3	1.7	1.3	2.2	1.4	1.0	1.0	1.7	1.9	2.1	1.9	1.5	1.6	1.9	2.0	2.9	2.3	1.8

Many of these cities and counties have limited resources with very little to no IT support. They are unable to provide adequate security tools and efforts to protect IT systems. The SLCGP is being utilized to address those concerns by providing much-needed tools to local entities.

With funding secured through the SLCGP and corresponding State appropriations, a comprehensive cybersecurity initiative has been deployed across 140 governmental bodies. This encompasses 23 counties, 94 municipalities, and 23 special districts. Consequently, endpoint security has been provisioned for over 26,000 devices, and cybersecurity awareness training, augmented with simulated phishing exercises, is being delivered to 31,000 local government employees. The whole-of-State program incorporates scheduled engagements with local leadership to deliberate on active projects and strategically guide the progression of State-wide cybersecurity initiatives.

The results have been extremely positive. We have blocked 7 major cyber-attack incidents in the last 6 months. I will speak of 2 of these.

Shortly before Christmas, the CIO of a local airport urgently contacted me about a cyber attack. Cyber criminals attempted to deploy ransomware on the airport's IT systems, which would have been disastrous, especially during the busy holiday travel season. Our CISO and Cyber Center team immediately worked with the airport's IT team to address the issue. Fortunately, SLCGP funds had provided security tools that were able to detect and interrupt the attack as it was happening. The common tooling and established relationships with local staff enabled a rapid response that limited the impact of the attack. As a result, the airport's service was not interrupted, and no ransom was paid.

Recently, a 9–1–1 dispatch center in Utah was the victim of a ransomware attack on systems that provide 9–1–1 services. SLCGP funds had provided security tools that detected and interrupted the attack as it was happening. Common tooling and established relationships enabled a rapid response that limited the attack's impact.

A WHOLE-OF-STATE APPROACH TO CYBERSECURITY

Utah's positive experience with this grant program is not an outlier. SLCGP has allowed States to further embrace a "whole-of-State" approach to cybersecurity, which NASCIO defines as collaboration among State agencies and Federal agencies, local governments, the National Guard, education (K–12 and higher education), utilities, private companies, health care and other sectors to address common technology and cybersecurity challenges. NASCIO has long advocated for a whole-of-State approach to cybersecurity. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly-defined role to play when an incident occurs.

Under this approach and with the flexibility allowed to provide shared services to local governments, States have been able to use SLCGP to provide vital technology services that many smaller communities otherwise would not be able to implement. While some States have elected to pass SLCGP funding entirely on to local governments, most have either provided service only or employed a hybrid approach of the 2 methods. According to one State CIO, "We are implementing (or trying to) a whole-of-State approach, recognizing that our weakest links often need the most support, particularly those under-funded entities that regularly deal with highly sensitive data."

States are also finding a wide array of applicable uses for SLCGP funding. According to the NASCIO 2024 State CIO Survey, cybersecurity training, endpoint detection and assessments are the primary focus for funds, followed closely by support for migration to .gov domains and security monitoring. It is precisely these critically important but attainable basic cyber hygiene measures that the grant was designed to address. Additionally, almost 100 percent of survey respondents stated that they would like for SLCGP to continue and cited the uncertainty around the program's long-term future as an impediment to further success. As we've seen in Utah, almost every State who has implemented funding from this program has seen some examples of tangible success in improving their cybersecurity posture.

Perhaps most encouraging, however, has been the spirit of collaboration between State and local leaders that the grant has fostered. One requirement to receive funding, the creation of a cybersecurity planning committee to guide how the money will be spent, meaning that these individuals are able to build relationships and trust that will allow them to respond more effectively and successfully to any cybersecurity attacks. Additionally, the "whole-of-State" approach has allowed local governments to learn about State services they can utilize, and for State technology leaders to understand where the greatest needs are.

It is this proven track record of accomplishment that led NASCIO and several other State and local organizations, including the National League of Cities, National Conference of State Legislators and National Governors Association to send a letter to the leaders of the House and Senate Appropriations committees urging them to maintain funding for SLCGP and to refrain from any actions that would undermine its continued success.

SUGGESTED IMPROVEMENTS

Of course, while we are encouraged by the program's accomplishments so far, not everything has been smooth sailing. Initial guidance was slow to be released, and States often received conflicting answers from CISA and FEMA to the same question. However, many of those early issues have been largely resolved.

As Congress begins considering reauthorization of this program, States have the following recommendations:

- Reduce matching contribution for State-wide cybersecurity efforts that provide shared services to local governments;
- Stabilize the matching formula across all years of the grant to simplify administration;
- Continue local government assessment requirements for participation;
- Elevate the shared services, whole-of-State option to ensure that States understand that this model is acceptable when administering SLCGP funds;
- Stress that local government cybersecurity assessments and other basic cybersecurity hygiene goals are undertaken before technology purchases are executed;
- Provide long-term stability and assurance for the program with a longer reauthorization.

CONCLUSION

The State and Local Cybersecurity Grant Program is not a "silver bullet" that can entirely solve our Nation's cybersecurity challenges. It does, however, help stake-

holders develop a solid foundation on which to continue to strengthen their defenses and modernize both their technology and processes. I look forward to discussing it today and answering your questions. Thank you.

Mr. GARBARINO. Thank you, Mr. Fuller.

I now recognize Mr. Kramer for 5 minutes to summarize his opening statement.

STATEMENT OF KEVIN KRAMER, FIRST VICE PRESIDENT, NATIONAL LEAGUE OF CITIES; COUNCILMAN, LOUISVILLE, KY

Mr. KRAMER. Good morning, Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for the opportunity to testify today. I am councilman Kevin Kramer from Louisville Metro Government in Kentucky. I serve as the first vice president for the National League of Cities. I am honored to speak on behalf of both my city and the 19,000 cities, towns, and villages represented by the National League of Cities.

NLC is committed to strengthen the Federal local partnership that supports our communities. Prior to my current role I chaired NLC's information technology and communications committee. I also work as a teacher at a small all girls high school. I appreciate this subcommittee's focus on reauthorizing the State and Local Cybersecurity Grant Program and I'm here to share both our local experience in Louisville and broader perspectives from cities across the country.

Local governments are frequent targets of cyber attacks. From both criminal organizations and nation-state actors. We are responsible for sensitive data, public payment systems, and critical infrastructure. When city networks are attacked, emergency services may be disrupted, personal data can be exposed, and entire communities can be impacted.

Recovering from these incidents often costs hundreds of thousands of dollars and hundreds of work hours. As the committee has noted in previous hearings, local governments face serious capacity constraints. This is especially true of small and rural communities. Of the 19,000 municipalities nationwide, over 16,000 have populations under 10,000 people. Many have no dedicated IT staff at all. Even larger cities often struggle to hire and retain qualified cybersecurity professionals. Yet, smaller size does not equal lower risk. Every community is vulnerable. Louisville Metro Government has received funding through the State and Local Cybersecurity Grant Program for 2 fiscal years. The most recent grant helped support the creation of the Kentucky Cyber Threat Intelligence Cooperative or KVTIC.

This is a new platform for sharing timely, actionable, cyber threat information among regional government and private-sector partners. We built it to address delays in the existing systems for threat reporting and communications. KCTIC allows anonymous threat data from cooperative members to be shared in near-real time. This grassroots, multi-sector effort strengthens the entire region's cyber resilience, not just Louisville's and it wouldn't be possible without this grant program.

The State and local cybersecurity program is a vital component of our national security strategy. It fosters State, local collaboration, builds awareness among local leaders and enables proactive

planning. But for the program to reach its full potential improvements are needed. First, the one-size-fits-all pass-through model limits efficiency. Larger jurisdictions like Louisville are capable of managing direct Federal grants and should be able to apply without going through the State. We urge Congress to create a complimentary direct funding track for eligible larger municipalities.

Second, the application process must be more accessible. Small communities face major barriers, tight deadlines, complex requirements and limited staff capacity. These are often the very communities that would benefit the most. Simplifying the application process and extending time lines would make participation more realistic for them. We are also encouraged by emerging models like multijurisdictional grants, managed by State and municipal associations.

These allow technical services to be delivered to many communities at once and approach far more efficient than requiring each town to stand up its own cybersecurity team. Just as most people take their cars to a qualified mechanic, small governments need trusted partners to handle complex cyber tasks. Above all, we ask Congress to reauthorize and fully fund this program with predictability and consistency. Without that, local governments are less likely to make the necessary investments in planning and assessment that leads to strong applications and long-term resilience.

Cybersecurity is a whole-of-Nation challenge, it demands a true intergovernmental partnership. The State and Local cybersecurity Grant Program is a cornerstone of that partnership.

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

[The prepared statement of Mr. Kramer follows:]

PREPARED STATEMENT OF KEVIN KRAMER

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 cyber threats.

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 coun-

try, 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 2 fiscal year cycles. The latest grant awarded allowed our community to do 2 main things. First, it allowed Louisville Metro Government to perform comprehensive testing of critical systems, such as life-saving applications, without reliance on third parties which is expensive and can take months to arrange and execute.

Second, it allowed Louisville Metro Government to take in and share critical cyber threat information with regional and State-wide 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 cyber attack. 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 maintenance 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 pass-through 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 pass-through 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 cyber attacks, 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.

Mr. GARBARINO. Thank you, Mr. Kramer.

I now recognize Mr. Raymond for 5 minutes to summarize his opening statement.

STATEMENT OF MARK RAYMOND, CHIEF INFORMATION OFFICER, STATE OF CONNECTICUT

Mr. RAYMOND. Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee. I am Mark Raymond, chief information officer for the State of Connecticut. I'm responsible for all the technology of 39 Executive branch agencies, including network and internet services for our K–12 schools, our libraries, our universities, and over two-thirds of the State's municipal governments. I'm an active member of NASCIO and the longest-serving State CIO in the country. This history has given me direct involvement with the long advocacy for dedicated cybersecurity funding.

The threats posed by criminal actors are numerous and unceasing. Each year cyber attacks become more threatening and the risks posed to residents become more dire. State and local governments serve as stewards of a civil society working to ensure community stability, predictability, and the well-being of our residents—these public servants are the teachers in our classrooms, the police officers who respond to distress, the doctors and nurses who care for our neighbors suffering with addiction. They protect the water we drink, the food we each and much more. All of these services however rely heavily on technology and data. However, the fast-growing cyber risks have found many jurisdictions unprepared. This program is a valuable resource in addressing this need. With this grant, Connecticut has expanded offerings to local governments. Equally as important is the spirit of trust the grant has fostered between State and local governments. Cyber incident responders are collaborating before attacks take place, instead of during them or after them. Preventing attacks is far better than recovering from them.

For the fiscal 2022 grant year we awarded close to $3 million, with more than $2.1 milion of that going directly to local governments. The awards for the fiscal year 2023 program year expected to be over $7 million in total with $4.3 million to local government.

One of the benefits of the program has been a systemic assessment of local government risks. Connecticut partnered with our National Guard to evaluate cybersecurity risks using the NIST cybersecurity framework. Sadly, only 27.7 percent of our municipalities were assessed at low risk.

These periodic assessments that are supported by this grant program ensure that the actions we take produce measurable risk responses. Those with high risks demonstrated a lack of vulnerability scanning, multifactor authentication, employee cybersecurity training, malware prevention tools, and incident response plans. This grant directly addresses those findings.

Fifty-one awards were made in Connecticut, of which 19 addressed incident planning in governance, 31 improved multifactor authentication and ransomware protections. The last award supported the Cyber Nutmeg which is a 2-day exercise where all municipalities and critical infrastructure operators are invited to participate. This unique State-level exercise raises awareness to the need to fill this gap. It exercises the incident plans that some are newly created and improves relationships that are needed when incidents occur. Unfortunately, these grant program funds for fiscal year 2022 covered less than half of the requested need. We plan to address this growing gap with the remaining grant year funding.

Though much has already been accomplished under SLCGP, more can be done and here are a few of our suggestions. First is the on-going dedicated funding for cybersecurity would be important, many local governments are reluctant to start a cybersecurity program without on-going funding to support it. Standardizing the matching percentage across the grant years would also significantly simplify grants administration.

Finally, making shared services a default position for States and local government to reduce the administrative burden required for each locality to sign on to the shared solution. This would reduce costs and improve State-wide efficiency. We strongly believe it is better to continue to improve this program rather than to allow it to expire. The grant improves our Nation's cybersecurity defenses, as State and local governments take on additional responsibilities for cybersecurity, supplemental funds will help meet this increased burden.

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

[The prepared statement of Mr. Raymond follows:]

PREPARED STATEMENT OF MARK RAYMOND

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 39 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 on-going 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.

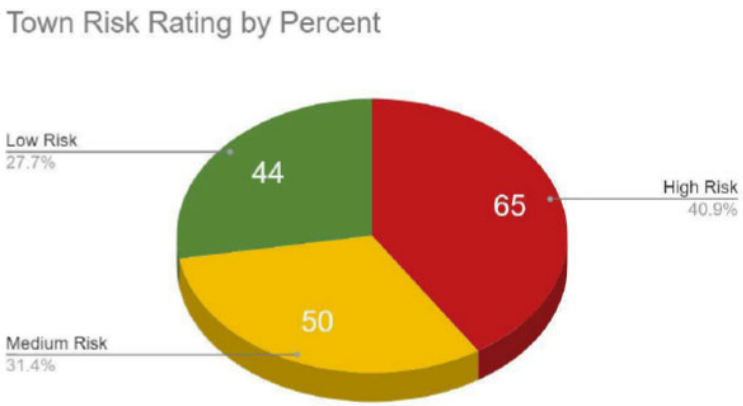
To that end, through the grant, we have expanded State offerings to local governments, including risk assessments, dot-gov domain expansion, multi-factor authentication, ransomware prevention software, employee training, and other critical services. Perhaps most important, however, is the spirit of trust 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 fiscal year 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 fiscal year 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 percent) 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 on-line 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 fiscal year 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 2-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 State-wide solution could be reduced. Flexibility to implement shared solutions, such as a State-wide 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 cyber attacks, 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.

Mr. GARBARINO. Thank you very much, Mr. Raymond. I hope the point about preventing is better than recovering, you know. Our county got hit and we were down for almost a year. So it is very important that you are all here today and getting this reauthorized and fixed I think is a very important goal that we all have. I'm really happy that we have Members to ask questions.

We're going to start with each Member and go from Republican to Democrat, 5 minutes of questioning each. An additional round of questioning may be called after all Members have been recognized.

I now recognize the gentleman from Texas, Mr. Luttrell, for 5 minutes.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Mr. Raymond, when it comes to local governments and their awareness of the grant programs and where they live and breathe and where they exist, how does that work? Does the Government itself reach down into these local governments? Which ones do we touch? Are we touching all of them?

Mr. RAYMOND. Thank you for the question, representative. They are all invited to the discussion. We have formed regional subcommittees that include representatives from State, local, school districts.

Mr. LUTTRELL. When you say regional subcommittees, can you elaborate on that, please?

Mr. RAYMOND. Yes, Connecticut is divided into 5 administrative regions so we do not have county government in Connecticut so it's just the State and then 169 municipalities. So we have organized our emergency response into 5 districts and so each one of those emergency management and cybersecurity groups have their own planning committee, all of the chief executives in emergency management and cybersecurity professionals in that group are invited to the table in those discussions.

Mr. LUTTRELL. So it makes it easier for the State to understand what exactly is happening in cybersecurity when it comes to the grant profile.

Mr. RAYMOND. Yes, sir.

Mr. LUTTRELL. Mr. Kramer, have you got something to add to that?

Mr. KRAMER. Louisville is the largest city in the State of Kentucky. We do have counties in the commonwealth. The grant that we are currently using came directly to metro government in Louisville.

Mr. LUTTRELL. Is every county aware of the grant system itself and how they can grab hold of that?

Mr. KRAMER. Those that are members of NACo, the National Association of Counties are well aware because NACo is pushing this out as an issue that they should be very much interested in working with.

In Louisville it is not just Louisville that's taking advantage of grant, though. We're the largest city in the State, we are also very near being on the river, very near Indiana. We are working across the entire region. We've reached out to the universities, both the University of Kentucky and the University of Louisville, we are working with the National Guard. So it's a program that goes beyond just what we're doing in Louisville. It captures a good part of our State.

Mr. LUTTRELL. Mr. Fuller.

Mr. FULLER. Excuse me, yes. So the city of Utah what we are doing——

Mr. LUTTRELL. City of Utah?

Mr. FULLER. State of Utah. Tools, training, and relationship building. So we are over 75 percent covered with all the cities and counties. We hope to get that closer to 100 percent as we go.

Mr. LUTTRELL. The entire State is aware of this.

Mr. FULLER. Oh, yes.

Mr. LUTTRELL. That's remarkable.

Mr. Huber.

Mr. HUBER. I have no comment. That is outside my area of expertise. I rely on these gentlemen. I'm a vendor.

Mr. LUTTRELL. Welcome to the committee, sir.

When it comes to the relationship between State and local government, would you say that the return on the investment from these grant programs are beneficial? I will start with you, Mr. Raymond, because you said you did not utilize all the assets that were funded, I missed the year.

Mr. RAYMOND. We had double the requests than we were able to fund. So we did not have any excess funds. We had double the requests in the first year of the grant program and we expect that to continue. So I think that does demonstrate both the awareness that we have across the State, especially for our municipalities and upwards—and we took very little funding at the State level. There is a division between what you can take at the State level and what is and almost all of the funds went to local governments.

Mr. LUTTRELL. But absolutely necessary because this committee is trying to maintain its footing when it comes to grant programs for cybersecurity, cyber threat. We need to hear from those on the other side to say, yes, this is an absolute lead because in my personal opinion, this is the next phase of evolution when it comes to warfare and protecting our citizens is absolute. As the meta verse is pulling, pulling or cutting or freezing grant programs currently I would hate to see this happen in such an important space.

Mr. Kramer, I'll go to you, if not, Mr. Fuller.

Mr. KRAMER. Thank you. I would argue that yes, it is essential. In Louisville we hired 2 people to do the work, we were hoping for 4. The work that needs to be done is broader than the work we are able to accomplish under the current program so absolutely want to see this going forward. The plan is to reach out again to the major universities in town and then ultimately to filter down even

to the public school systems. It is amazing how much data is held in the school systems and how much that data is compromised.

As everyone knows, the bad actors are looking for the easy access. So we're doing our best to reach down to the level where we can improve security at that lowest level.

Mr. LUTTRELL. Mr. Chairman, I yield back. Thank you.

Mr. GARBARINO. The gentleman yields back. I now recognize the Ranking Member, Mr. Swalwell from California, for 5 minutes of questioning.

Mr. SWALWELL. Thank you.

Councilmember Kramer of Louisville you have one of the most important jobs here, you are protecting the Nation's bourbon supply so thank you. I know our Chairman and many of my colleagues thank you. But you did, in all seriousness, mention the weakness of the program as it exists right now, which is it doesn't have much agility or maybe you said bandwidth to understand the differences between sizes of cities. Like, how would you structure a future reauthorization to better reflect that, and better target where the need is?

Mr. KRAMER. Thank you for the question. I really appreciate that. The first bit of the answer is we need to recognize that larger cities like Louisville, for example, we do have the resources. We have a person on staff who his primary responsibility is cybersecurity. But we're a half-an-hour drive from Elizabethtown—there was a movie made about that place—it is a fairly small town out in the middle of bourbon country. They don't have the resources to do this. But we do have a very active stately city, an organization of municipalities.

Allowing the grant to go through them instead of through the State would assure that that money actually made its way to local governments and it also allow the State league to work together with those other cities and hire a person that would be able to work with all of them and not just with one city like our own. Again, it reaches into the school systems. There are some school systems in the State of Kentucky that the highest-paid positions in the county are in the school system.

I just want to drill home that's an area that I think folks overlook. There's a lot of data that's handled there and we need to do the best we can to reach out to that community as well.

Mr. SWALWELL. Absolutely.

Mr. Raymond, can I ask, as somebody who has administered millions of dollars of these grants to many jurisdictions, municipalities, agencies, what are some of the weaknesses that you've seen among some of the recipients?

If you had a new tranche or a new reauthorization, what have you learned from this that makes a candidate more eligible or makes a candidate least eligible as you're thinking about where these funds should go?

Mr. RAYMOND. Well, admittedly the program did have a slow start, right? I think any kind of new grant program, the clarity around getting people to understand what it is to be eligible and what people really needed within their environment was probably the most difficult challenge for us.

Again the assessment, the cybersecurity assessments that were part of the first year were absolutely critical for building, for all of our municipalities and understanding of what their risks were and how we would address it. I think it goes to the earlier question of, did they know? When we have these assessments, they now know.

So I would say that continuing that to demonstrate the improvements would be absolutely critical. For additional funding, I do think that—I understand the desire in the construct of the program to have—to wean States off the program with the declining match or the increasing State match. However, that's complicated with the change in the funding as well. I think having a stable match over the life of the program makes it far easier to administer as people are working across the different grant years.

Should the desire be to still shift some of that burden back to the States through the funding, you can do that through the overall funding of the program and not the mix of the 2. I think that we had a lot of people applying for the first year and a 90 percent reimbursement rate and then we're looking at will we get that same kind of participation as the rates fall and local governments' budgets remain tight.

Mr. SWALWELL. Thank you. I yield back.

Mr. GARBARINO. The gentleman yields back. I now recognize the gentleman from Tennessee, Mr. Ogles, for 5 minutes of questions.

Mr. OGLES. Thank you, Mr. Chairman, to the witness.

I believe strongly in federalism, fiscal responsibility, the importance of empowering local communities and not expanding the bureaucracies of, quite frankly, the Federal Government.

As we assist the State and local cybersecurity grant program we need to ensure that our limited Federal resources are being used effectively are actually reaching the communities most at risk. I say that in the context of being a former county executive in Tennessee, serves as the CEO of the county.

So I can attest to the fact that some of these pass-through grants administered by the States were incredibly important to my county which is a rural county, emergency services, fire and cyber were all my departments.

So again, I get your perspective on the stable match because again as a rural county where we have limited funding mechanisms and quite frankly an ever-growing school system where there is a friction there of how do you fund these mechanisms which, as my colleague stated, the future of warfare is on the cyber battlefield.

That being said, Mr. Huber, you worked to secure systems against the threat from Volt Typhoon, the CCP, that group of hackers who both have sophisticated abilities and specialized in targeting the most vulnerable points in its target system.

In your testimony you mentioned an attack on Littleton Electric and Light & Water Department in Massachusetts. My district and across the country where a diverse range of electric providers, large corporations, rural providers as I mentioned.

In your experience how strong is the awareness of cyber threats among smaller, less-resourced organizations that provide critical infrastructure? Again, I go back to Tennessee, but probably much like rural Kentucky where we have a patchwork of these smaller

communities, where we are scrapping for resources, to figure out how do we quite frankly protect not only our infrastructure but our citizens, sir?

Mr. HUBER. Yes, I thank you for the question. So having had the pleasure of working with—that the IT person was the IT person, and the database administrator, and the assistant administrator, and responsible for security, at a part-time job.

So as you might imagine, any administrative burden that might be involved in applying for the grant would be significant for an entity such as that smaller size. But make no mistake, those smaller rural entities that could be the hydro station that fuels a larger municipality. That's a national security and economic impact in the region.

So as we heard from a gentlemen here educational awareness is key to educating those folks who have probably dual roles, or multi-hat roles from protecting that piece of critical information from nation-state attackers.

As one who has been in the trenches and a National Guard member in Title 32 and State Active Duty supporting State credit infrastructure components. There is a significant shortage of resources and knowledge about nation-state-level attackers.

So think it is important to recognize that this funding is key in raising the bar of foundational cyber controls for all of those entities.

Mr. OGLES. I want to focus primarily with the other 3 witnesses on rural communities. One of my concerns, again my background coming from a rural community is that competition that you see between say a Nashville and my community. But yet from an assessment standpoint, I would argue some of your rural communities are your most vulnerable points of intrigue.

So how do we make sure that we're prioritizing, basically—take size out of it for a moment—but a needs assessment, understanding that again whether it is distribution of broadband, whether it is protecting points of entry, et cetera. Mr. Fuller.

Mr. FULLER. Thank you very much.

Let me just say I really appreciate your comment that these attacks are very much like war. This committee knows very well that we live in a very, very dangerous world and we were constantly under attack including our smallest and most rural community.

So with the program that we rolled out, we rolled out tools that all of our communities, including the rural communities and the most rural that don't even have section IT resources, we are able to make resources available to help them install those tools and then we are also able to provide training for those people. So we're absolutely committed to getting this program to our small cities and counties in special districts.

Mr. OGLES. Mr. Kramer.

Mr. KRAMER. Thank you again, it is a great question.

I think one of the things that we need to recognize is it a matter of how quickly we share that information as well. When a cyber attack happens what they are trying to do in one place, one community is likely happening somewhere else. Again, I think the smaller communities, the rural communities where my colleagues have testified that you've got a person who has 3 different jobs.

If they aren't aware of what to look for it makes it much more difficult. They often don't find out until it is too late. So one of the things we are hoping we can get the Federal Government to do is recognize that they collect up a lot of data about cyber attacks, but they collect it up and hold it.

It would be very useful to us at the local level if as soon as they knew about a cyber attack they shared that information with entities as quickly as they could so that folks at the local level could start looking at their own systems and see if someone is trying to get in the same way.

Mr. OGLES. Yes, sir. I am out of time, but Mr. Raymond a final thought.

Mr. RAYMOND. I would just say that we view cybersecurity as a team sport. We view those that are better-resourced in a good position to help those that aren't. So we do have municipalities who help each other, larger ones helping smaller ones and smaller ones who are relying on the State to help deliver services.

We do run all of the network services so it provides a unique ability for us to provide specialized security services to everyone in our jurisdiction, which is one way to make the limited dollars we have left to go a lot further.

Mr. OGLES. Thank you, to the witnesses. Mr. Chairman, apologies for going over.

Mr. GARBARINO. Of course, no problem. The gentleman yields back.

I recognize the gentleman from Rhode Island, Mr. Magaziner for 5 minutes of questions.

Mr. MAGAZINER. Thank you, Mr. Chairman.

The State and Local Cybersecurity Grant Program is an essential resource to help States and municipalities protect themselves against cyber attacks. This grant program helps secure critical infrastructure like schools, hospitals, electric grids, water systems.

My home State of Rhode Island has been instrumental in providing cybersecurity training for example for staff at State agency municipalities so they can better protect taxpayer data, securing schools and academic institutions from ransomware attacks and protecting critical infrastructure from being infiltrated by hackers.

I am concerned by reports of potential delays and cuts to these grants by the Trump and Musk administration. I'm glad to see that at least in this subcommittee there appears to be bipartisan support for continuing the program in a robust form.

But you would forgive us for being concerned because in addition to the reports of delays, we have heard that the Trump and Musk administration has been firing staff at CISA and at FEMA, the 2 agencies responsible for administering this program.

We have also heard from Secretary Noem herself that she plans to "eliminate FEMA and significantly shrink CISA." She said that in her Senate confirmation hearing. This would be a tremendous mistake. The threats that we face from foreign maligned actors, from criminal organizations, to critical infrastructure, to our cybersecurity are a mix.

The Chinese are working overtime putting tens of thousands of people toward trying to infiltrate every system, even in the smallest towns in this country, same with the Russians, same with the

Iranians, the North Koreans, and of course criminal cyber gangs as well.

We've had significant breaches in Rhode Island as a result. This is not the time to take our foot off the gas as the Secretary said was her intention during her Senate confirmation hearing. Unfortunately this is part of a pattern because when she was Governor of North Dakota, Secretary Noem was 1 of only 2 Governors in the entire country who refused to accept State cybersecurity grants in 2022.

Her administration called it wasteful spending. In 2023, yet again, she was the only Governor in the entire country who refused these grants for her own State. Of course we have seen that the administration is not off to a great start with its own cybersecurity practices, with service members' lives being put the risk from confidence information being discussed in an unsecured group chat.

Of course Elon Musk's army of unvetted interns going through everybody's data with very little transparency. But given that backdrop, it is more important than ever that Congress send the message that cybersecurity still matters to us, that we do not consider it to be wasteful spending, and particularly we want to continue to support States, municipalities, utilities in our home States with this program.

So I have limited time, but Mr. Fuller, can you elaborate on any reports of delays, cuts, or pauses to this program? What have you seen so far? What would the negative consequences be?

Mr. FULLER. Thank you. I appreciate your point that there is a lot of bipartisan support for this program to continue. Certainly the risk doesn't take politics into account.

One of the concerns we have about the program is some of our States chose not to participate because they were afraid the funding would not continue on and they were afraid to launch a program that might then get cut. That created some hesitation for some States.

First, we're all in with the program. It has been extremely beneficial, that's been my testimony, we blocked 7 major attacks in the last 6 months alone.

So we would hope that we could extend the funding, could be extended by Congress without delays. Those delays could cause serious problems in adoption of the program.

Mr. MAGAZINER. Thank you. Mr. Raymond, even if eliminated and CISA is significantly cut as Secretary Noem has promised, what impact would that have on the ability of your State and others to maintain strong cybersecurity and take advantage of programs like this one?

Mr. RAYMOND. I do believe that FEMA and our emergency management in Connecticut along with CISA on the securities side have been great partners with us on this cyber battle. State and local governments are not prepared to fight this kind of cyber engagement with foreign nations.

I would say in combination with the reduction to the MS–ISAC and CISA support additional responsibilities are falling on the States to fight these battles.

Should further CISA reductions or FEMA reduction for that matter be put in place, I would say it would diminish our ability to

help the municipalities that are part of our jurisdiction and defend on behalf of the State.

Mr. MAGAZINER. Thank you. I'm over time so I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize myself for 5 minutes of questions.

Gentlemen, we have heard from you all today. There is definitely a need for the program. I want to focus on No. 1, has it been successful so far? No. 2, what changes would we make?—and you have all suggested a couple.

Mr. Raymond you started by saying when you first did the—in your statement there was 27 percent of the municipalities were low-risk so 73 percent were not low-risk. Now that this program's in place, have you done another review? What number's low-risk now?

Mr. RAYMOND. We are currently doing the reassessment now. We do not have an updated set of numbers on this. We do know that the implementation of the 51 grants that we have would directly raise the ratings and lower the risk for folks around.

Mr. GARBARINO. Mr. Huber, you're a vendor so you're dealing with all these municipalities. You know what they are using, what they needed. Can you please just describe what these grants have been able to help some of the municipalities that you've dealt with, like, what systems have been put in place? What they had and now what they have. I think people really—we need to hear the actual benefit of what you've done with this grant money.

Mr. HUBER. Sure thank you for the question.

Yes, so one of the first foundational components any cybersecurity program is having awareness of what you have. You have to know what you have to be able to defend it. It sounds easy, a significant challenge for most organizations, even mature organizations, that's a challenge. To understand the breadth of the footprints certainly at the State level, let alone rural areas as well.

So what we've seen folks do is deploy solutions without understanding what they have in their purview, what's exposed. So to the gentleman's point regarding risk assessments. You have to know what you have to conduct that risk assessment so that is step No. 1. We have seen them deploying that successfully.

Then you want to take that just a step further. Now I know what I have what am I vulnerable to? What misconfigurations, weakness, vulnerabilities do I have there? How do I prioritize those from a response perspective? Because I have limited resources to go and mitigate and reduce those risks.

So now I'm looking at what are my resources available to go and reduce the risks across the entire enterprise without regard to the size of the municipalities evolved, right? Because it could be when they do these risk assessments some smaller or rural regions might have the highest risk compared to larger metros. What we have seen successful organizations assess what they have, being able to analyze them and look for exposures across the attack footprint and then focused on a prioritized cause addressing vulnerabilities.

Mr. GARBARINO. That's great. So you are using the grant money to map the system because and now—it a multi-year grant so they are mapping their system, they are funding out what doors need

locks and now they are implementing it and using technology to protect those doors into their system.

Mr. HUBER. Yes, I think a great point is sustainable funding, you know, I hate to use this example, some people when they wake up they have a day job, it is not to fix vulnerabilities, that is not their job. Their job is to make the systems run.

They go patch the systems and they are like, mission accomplished, we're done here and tomorrow morning you get up and read the news and you are, like, more vulnerabilities you have to do this again.

It is a hamster wheel—so people have to have not only resource and fun for that, it is now a part of your job or some percentage of your time beyond what your day job is. People need to understand that's how life is.

Mr. GARBARINO. Thank you very much. So under the grant program there is some requirements in the law, one of them is for there to be a submission of a cybersecurity plan. This is for the 3 gentlemen on the right who actually had to determine the cybersecurity plans.

There's a lot that's going to be part of it. What is working as part of the plans, is there something that we should include that is not in it or is the law overburdensome by including too many things in the plan that's not necessary? What do you all think? Mr. Fuller, we can start with you.

Mr. FULLER. Thank you. I think the good thing about the plan is that it gave States some flexibility to each create their own plan. You can see between Connecticut and Utah, 2 very separate plans, where they primarily put funds down to local entities and we primarily provide tools, training, and relationships down to local entities. So I feel like that part of the law was successful good.

Mr. GARBARINO. It should not be changed.

Mr. Kramer.

Mr. KRAMER. I am going to leave that to the folks who actually do the cybersecurity stuff.

Mr. GARBARINO. OK. Mr. Raymond.

Mr. RAYMOND. I would say the formation of the cyber plan was really hopeful to focus in a structured way on what the risks were and what we can do together to lower those risks. There was a tremendous amount of collaboration in the development of the plan which I think furthered the mission of hey, we're all in this together and hope to get the message out to all of the municipalities that this was important for their success.

So I think the combination of collaboration and structure in those plans and the direction that set was very hopeful for State-wide efforts.

Mr. GARBARINO. Sounds like that part of the statute is something that should not change.

OK, we're going to start a second round of questions. I now recognize the gentleman from Texas, Mr. Luttrell, for his second round.

Mr. LUTTRELL. Mr. Huber, I think you hit the nail on the head explaining exactly how the process should work. Is that even a possibility or a probability, remember you're talking to the United States of America right now. I want you to think about that I don't

where you're from. Kentucky, I'm from Texas, obviously. A little bitty town.

We hate the Federal Government. I can throw that out there. Honestly, we don't want them in and around us at all. However, with the threat or the risk to threat when it comes to cybersecurity space, how do we make this work? The plan that Mr. Raymond laid out piggy-backs exactly what you said.

But we have to touch every single person in the United States of America and I can assure you the 4 of you sit in front us, you're not the first 4 that's ever sat in front of us and laid this out. This is almost the simplest question, how do we fix this problem or is it a possibility?

We can just keep talking about it all day long. We can keep funding these grants and throwing it out there and we're just going to get attack after attack. You said the problem is when the attack happens, we're retrospective. It's a done deal. Then we have to raise awareness to those that didn't get hit. Who's doing that?

Well I've had CISA come out to my district. I've had the FBI come out to my district and talk to the nursing homes and schools. Guess what? The things they laid out, a month later, something else showed up. Literally, how do we fix this?

Mr. HUBER. Yes. Thank you for the question. Great question. We have to raise the bar across the board. There is foundational cyber——

Mr. LUTTRELL. What does the bar even look like?

Mr. HUBER. I think in this cybersecurity——

Mr. LUTTRELL. You and I are going to have a pretty good healthy debate here in 3:16. Every time—you see where I'm going with this.

Mr. HUBER. I do, absolutely. This cybersecurity framework provides excellent foundational controls, but to your point, AI was not on my list of risk 3 years ago, and now it is. Guess what we're doing. We're developing those foundational components for artificial intelligence and how we defend and how we detect for that type of capability, so we're always going to be in that race of emerging technology, unfortunately for us.

What those foundational components still hold true for the vast majority of threats that exist today, and I think what we heard is very key of getting the message out, which is that communication and collaboration, whether that's through JCDC, under CISA, or whether that's through some of these fusion centers we heard of at the State level where they're disseminating information, it is a collective sport at the end of the day, and we all need that information to be able to respond as quickly as possible.

Mr. LUTTRELL. The sheer processing speed, we're past excess scale computing. Magnolia, Texas can't defend against that. We have a—we have nefarious actors that have the computational capabilities to destroy a country. How do I protect District 8 in Texas?

Mr. HUBER. I think—and this is not normally how you start the security program, but you should start with instant response. You need to have search capabilities and resources to respond to an incident. To your point, unfortunately, it will happen. We have data that shows it will happen to even the most mature organizations,

so having those capabilities, a lot of times those search capabilities, and I've been in this role, they come from the National Guard, they come from CISA and other organizations to provide us intelligence we don't have to collectively respond as an industry, and that also raises the bar.

Mr. LUTTRELL. I mean, how much—I can't even repave the roads in my forest right now, so now here we're talking about dollar bills, and I can only imagine that protective layer is going—help me fix this problem. I mean, what——

Mr. HUBER. Yes. There's certainly data points available of known exported vulnerabilities. It's something we use in an industry to prioritize. Like, we know these are actively exporting against these organizations. You want to make sure that when you're applying resources against the problem it's a prioritized approach, whether it's through the program assessments that these organizations complete to identify the highest risk or whether it's vulnerabilities that you see day-in and day-out to prioritize those first.

I know within Tenable we have data that says, unfortunately, if a new vulnerability comes out that affects major operating systems as an example, it takes most organizations a few weeks to address those vulnerabilities. By the way, they only fix about half of them during the course of that 2 weeks, so there is a known exposure that we all accept. Like I said, to foot-stomp this, having a good response plan of how you coordinate reaction to those events becomes critical.

Mr. LUTTRELL. Thank you. I yield back, sir.

Mr. GARBARINO. Gentleman yields back. I get the gentleman's point about there might not be a way to stop this, how do we stop this? I don't know if we can stop it, but being able to respond and get things back on-line I think is what—is at least part of the goal here.

I now recognize the gentleman from California, the Ranking Member Mr. Swalwell, for his second 5 minutes.

Mr. SWALWELL. Thank you.

I'd welcome the opportunity with the 4 of you here to give us a real-time update on the threat environment and what you're seeing as to the type of the attack, the ask of the attack, if it's ransom wear, your ability to work with the Federal Government, for example, the bureau when an attack occurs, and the origin of the attack. Is it still primarily Russia, eastern Europe, criminal gangs for ransomware? Then as far as phishing attacks and intellectual property theft, is that primarily China?

So, Mr. Huber, start with you. If you each spent about a minute on this I think we would get a good cross-sector update.

Mr. HUBER. Yes. I think it's heavily dependent on the sector the entity operates in. You do see all those actors across all sectors, and unfortunately, you know, it has become easier. There's things such as ransomware as a service as an example. You can buy access to systems and companies at your will without having to conduct any actual tax themselves, and then, of course, we always have the nation-state actors.

Mr. SWALWELL. So it's like investing in the stock market. You just, like, buy an index fund of ransomware attacks?

Mr. HUBER. That's exactly it. So if I wanted to compromise your machine, I might buy access from somebody who already has access to your machine, so I'm going to actual conduct the activity myself.

Mr. SWALWELL. Sorry. Continue.

Mr. HUBER. So I think we're seeing a mixed bag, and the problem becomes to Congressman Luttrell's point is, you know, trying to defense against all of those different types of actors, whether it's, you know, financially-motivated, ideology-motivated, nation-state-motivated, they all have different intents for what their targets are, so you have to understand to a great extent what your attackers look like, and that's, again, where some of that information through law enforcement or CISA or JCDC is very useful.

JCDC as a part of CISA, we used—they coordinated responses for log per day, massive vulnerability. It affected the economy and the world for that matter, one of the largest ones of my career. They did a fantastic job of sharing what works, what doesn't, and getting us intel quickly that we can action.

Mr. SWALWELL. Great. Thank you.

Mr. Fuller.

Mr. FULLER. Thank you so much for the opportunity. So the types of attacks, first of all, the end-users are typically the biggest vulnerabilities, so we see things like phishing attacks, business email compromise. I'd like to give you a very specific example that we just had the last few weeks. Utah is an alcohol-controlled State. We have retail stores that sell alcohol.

We had criminals calling these liquor stores representing themselves as members of the government and saying that they need to change settings in their credit card readers. The credit card readers, they were trying—the settings they were trying to change were trying to make it so the card haven't have to be present, it was a blatant attempt to try to hack the credit card readers of our liquor stores.

We've seen just in the recent past a business email compromise has been very damaging. We've seen—they try to do things like convince State employees to change bank routing numbers to redirect funds so it goes to the criminals instead of to the place it's supposed to go. The primary attackers come from Russia, China, North Korea, Iran, and we've seen quite a bit from Nigeria.

I would also just mention that to some of the comments before that with artificial intelligence technology, unfortunately, I see the problem getting worse, not better. It used to be with phishing type emails, you would see typos, incorrect grammar. You could kind-of spot that something wasn't quite right.

Unfortunately, the criminals know how to use artificial intelligence as well. We just had an incident where we had over 400 phishing emails, every one a different subject line, every one a different text, all written beautifully. Unfortunately, all bearing malware that could compromise systems. So unfortunately, the world is getting more dangerous, not less.

Mr. SWALWELL. Thank you. That's helpful.

Councilmember Kramer.

Mr. KRAMER. So in talking to James Meece, our cybersecurity guy back home, he mentioned some of the same things that have been testified to here. There are certain localities that we know

when something is coming in. It's probably suspect just because of where it's coming from.

In 2023, we had a nation-state cyber actor get access to one of our network devices through a provider's chat. You wouldn't think that's a big deal, but in the process of chatting back and forth with other folks on that same system, they were able to get passwords, user names, and later were able to go in and try to—they got into the network where they could see what was going on. Fortunately, we were able to catch that before they were able to do anything, so it only cost us about 100 hours to fix it. We were grateful.

Typically, these things—the problem is, as you guys well understand, if you don't spend the money up front to know what's coming, you're going to spend the money on the back end. You know, we talked earlier about local governments and rural communities. The real issue there is a lot of the rural communities, they don't have the resources to spend up front, and so they don't, and you don't have a choice about spending on the back end.

Mr. SWALWELL. Time expired. Would you indulge me and allow the CISO from Connecticut, please, Mr. Raymond.

Mr. RAYMOND. Thank you. I would say very similar answer. We're seeing global interest in things that we do. If we put a new device on a network, 5 minutes it is being scanned by someone, so they are looking for the vulnerabilities that were being described for scanning earlier.

The threats are data exfiltration, stealing of data, of intellectual property, ransomware, extortion of data, business email compromise. It's a phishing targeting of leaders for passwords, and those kinds of things are very common things that we see.

Mr. SWALWELL. Thank you. That was helpful across the board. Chairman, I yield back.

Mr. GARBARINO. Gentleman yields back. I'm going to continue along my line of question from before about changes. CISA and FEMA's role, are they good partners? Are they the ones who should be running this program? I mean, has it worked? Has it not? Jump in.

Mr. FULLER. If I may, Mr. Chair, CISA has been an outstanding partner for us. We're really grateful for them and their commitment. We use them in a number of ways. They are active members of our cyber center as well as the Federal Bureau of Investigation. Those relationships are extremely important. When a bad thing happens, it is so good to be able to have experts to reach out to and know who to call. CISA and FBI help provide that role for us. We're very grateful for their support.

We also use CISA's services to do cybersecurity assessments of each of our agencies in the State across the board. We do that once every 3 years for all agencies, and they've been a tremendous partner for us.

Mr. GARBARINO. Mr. Raymond. Kramer.

Mr. RAYMOND. Yes, I completely agree. The CISA team has brought great leadership and insight and expertise in terms of both what we can leverage. But to the earlier question, they've been fantastic in getting out to the local governments in being—helping them raise the understanding of what's available and how they need to be thinking about it. FEMA has been sort-of a back office

partner for the grant administration. I'd say less active in the delivery of the technology, but they've—they've also been a great partner.

Mr. KRAMER. I'd say baseline been a great partner. Really happy about what's going on so far. The one-size-fits-all approach has been somewhat limiting. It limits some of the efficiencies. We would hope that Congress would create a more direct competitive grant fund with SLCGP for larger municipalities who can afford to take care of that on their own. I think that would be helpful.

The other is we recommend an application process to be simplified to encourage participation by some of our smaller communities.

Mr. GARBARINO. Simplified how?

Mr. KRAMER. The reporting processes are somewhat burdensome. Again, keep in mind, and some of my colleagues have already testified, very often these aren't full-time employees who are focused on, (A), applying for grants in the first place, and (B), just the technical nature of it alone. So if we could make it such that some of our less technical folks who are responsible for these highly technical responsibilities would be able to report more easily.

Mr. GARBARINO. Currently, Louisville—the city of Louisville has to go through the State to get its grant, correct? It's administered by the State?

Mr. KRAMER. I don't believe so. I'd have to check. I think ours came directly to metro local, although it may have come through the State. I'll withhold on that one.

Mr. GARBARINO. But you're saying part of this pot of money would be—instead of having—it might be worthwhile to have some of the larger cities and municipalities be able to go directly to——

Mr. KRAMER. Yes.

Mr. GARBARINO. Directly to FEMA to get—have some of the grants come instead of——

Mr. KRAMER. Yes.

Mr. GARBARINO. OK. You mentioned something about for rural, the cost. They can't even come up with a cost share. How would we fix that?

Mr. KRAMER. Again, I think that the program the way that it's designed, if we could get that more quickly, more easily to municipalities, to the—and again, we talk about cities and rural, municipalities are still in those rural areas. They're just much smaller municipalities.

In the State of Kentucky, and all the States, actually, there's leagues of cities, and the Kentucky League of Cities has been awesome to work with. It would be beneficial to local governments if the grant money were funneled or moved through that organization. They're more directly connected to what's going on in cities than the State is.

Mr. GARBARINO. OK. Mr. Raymond, Fuller, you both have rural areas. What could we do more to help there? Because, again, those are the municipalities that don't have the expertise, even though the Pivot Act the Chairman is leading would put—would allow people to hire and be part of the service. That's great. Nice little plug for the Chairman's bill. Hopefully passes, but go ahead.

Mr. FULLER. Mr. Chair, so I felt like it was kind-of ingenuous to run it through the States, because 80 percent was—80 percent of the funding came through the States, but 80 percent of the funding to go to locals, and that allowed us, the State, to directly help those rural cities and counties and give them the help that they need.

In some cases, we believe even to hire technical resources to help them implement the endpoint software, and we've been able to provide the training that they wouldn't have otherwise needed to do, so we've been able to—we as a State have been able to make it super easy.

We've just packaged it up and given it to them and even helped them implement it, so the way it's worked for us has been beautiful.

Mr. RAYMOND. I would add that the match allows for a waiver, depending on certain financial conditions, so I do believe that if people can't come up with the money to meet the match, they have a way to respond to that. However, I think people have been reluctant to use that in the expectation that that will slow down their award or perhaps not get it—it wouldn't be granted the match. So I think there's some trepidation for people to put in for that match waiver that's preventing some of the uptake of it.

Mr. GARBARINO. Wonderful.

Mr. Huber, you mentioned something in your opening statement that lowers the cost-sharing requirements. Is that—did you say that?

Mr. HUBER. I did, yes. I think there was opportunity certainly with State municipalities where it makes sense to provide shared services, so it increases the ROI for those services provided. As Mr. Fuller mentioned as well, you have expertise at the State level that can also be shared. They can hire additional resources there, so you have a known capacity providing resources to certainly rural and municipalities. I think that makes them more effective.

Then the cost-share component, which I mentioned earlier is, like, you don't want to put so much pressure on a small organization that doesn't have somebody whose full-time job applying for grants trying to do that, right? Justifying that resource to do that. You want to put them in the best position to be successful, to deploy the technology to protect the organization.

Mr. GARBARINO. Wonderful. I'm out of time, but I'm the Chairman, so I'm just going to ask one more question. So now we've had this hearing. It's our job to come back and to reauthorize this if we want to make any changes, so you're all the experts. You've all been dealing with this bill or this program. If you could all have—I want to hear from each one of you. If there was one change or fix made to this, what would it be? We'll start with you, Mr. Huber.

Mr. HUBER. I think you'd want to ensure that there's harmonization of any standards and compliance. You want this to be a cybersecurity exercise, raise the bar for cybersecurity, not a compliance exercise. Simple as that.

Mr. GARBARINO. Thank you.

Mr. Fuller.

Mr. FULLER. I would just say continuity of funding. That would be the main thing. People feel hesitant that if the funding is not going to be there that they're going to start in with the program

and then the funding gets cut and then they are left holding the bag, and that makes them hesitant to adopt.

Mr. GARBARINO. So the authorization should be longer than 4 years.

Mr. FULLER. Yes, please.

Mr. GARBARINO. OK.

Mr. KRAMER. I concur with both of my colleagues. Then I would add back in what I mentioned a moment ago. For large municipalities, if we could apply directly, I think that would be helpful. Then allow that organizations like municipal leagues would have an opportunity to work together as well.

Mr. GARBARINO. Mr. Raymond.

Mr. RAYMOND. I would say that on-going sustainable funding and then on-going assessments. You cannot manage what you don't measure, and so understanding what that cyber risk looks like is critical to this on-going success.

Mr. GARBARINO. Great. Well, I want to thank the witnesses for their valuable testimony today and the Members for their questions. The Members of the committee may have some additional questions for all of you, and we would ask that you all respond to these in writing.

Pursuant to committee rule VII(E), the hearing record will be held open for 10 days. Without objection, this committee stands adjourned.

[Whereupon, at 12:43 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ROBERT HUBER

Question 1. Are you aware of any instances in which the State and Local Cybersecurity Grant Program (SLCGP) has not been fully utilized in a given fiscal year? If so, how can we eliminate waste?

Answer. Response was not received at the time of publication.

Question 2. What challenges do States face in implementing SLCGP funds?

Answer. Response was not received at the time of publication.

Question 3. The SLCGP's statutory authorization permits the Secretary of the Department of Homeland Security (DHS) to take action to ensure compliance. How has DHS—or the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA)—ensured compliance with the grant program's requirements?

Answer. Response was not received at the time of publication.

Question 4. On average, how long does it take for a State or locality to start a cybersecurity program?

Answer. Response was not received at the time of publication.

Question 5a. Of the States and localities you have worked with, how many of them opted to apply for SLCGP funding as a multi-entity group?

Answer. Response was not received at the time of publication.

Question 5b. Was implementation of multi-entity group projects smoother or more challenging? Please explain.

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ALAN FULLER

Question 1. In reviewing your Cybersecurity Plan, did the Cybersecurity and Infrastructure Security Agency (CISA) help ensure your plan was implementable and reflective of the needs of your State? Please explain.

Answer. Yes. Initially, CISA provided us with guidance, resources, and possible templates to use in the creation of our Cybersecurity Plan. Those resources were aimed at ensuring we had a good, successful, and usable plan. We were required to submit our completed Cybersecurity Plan to CISA for review and approval prior to the submission of any projects or receipt of any funds. CISA reviewed the plan to make sure that it seemed reasonable and implementable. As part of the plan, we performed some assessments and looked at information from cybersecurity audits and surveys to point our plan toward what was needed in Utah as requested in the instructions for creating the plan. In the third and fourth year of the grant, we are required to review the plan and submit any changes for review and approval by CISA. Our understanding is that CISA is reviewing the plan to make sure it and future spending of grant funds and projects meet the goals of the grant requirements, are reasonable expenditures, and can reasonably be implemented to improve cybersecurity in the State. CISA personnel have been a valuable resource during the cybersecurity planning phase and throughout the SLCGP process.

Question 2. Are you aware of any instances in which the State and Local Cybersecurity Grant Program (SLCGP) has not been fully utilized in a given fiscal year? If so, how can we eliminate waste?

Answer. In Utah's case, there are no instances where the SLCGP has not been fully utilized each year. We have also not heard of any instances outside of our State. The parameters and guidance of the SLCGP give sufficient latitude in the time frame for spending and using the grant funds as intended. Since there is a several-year span in which to expend each fiscal year's funds, it provides the appropriate time to plan and implement good cybersecurity programs properly. If the time lines were shorter, it could lead to pressure to expend funds too quickly and without proper planning.

Keeping the current system in place, where the State receives the funds and can administer the programs and award subgrants, provides an excellent process to eliminate waste. There is strong oversight of the grant and expenses, a set focus for helping locals as percentages of the funds must be expended on locals, and an ability to purchase products at a mass scale to save money and ensure that they are being provided to as many entities as possible. If other entities within the State could apply directly for funds, it could cut into the ability to use economies of scale, create consensus and collaboration on cybersecurity projects, make it so smaller communities who need help were not served properly, and manage projects to ensure an effective distribution and implementation, which in turn would lead to waste. In addition, the SLCGP has guidelines to direct the spending of resources specifically on cybersecurity to avoid wasteful spending.

Continuing the program can eliminate the waste that occurs with prematurely starting and stopping the implementation of programs.

Question 3. Can you please describe how you track funding to ensure that the SLCGP's allocation requirements for local and rural entities are met?

Answer. With Utah's model, we have committed to ensuring all the funds go to help local governments and rural entities. The 20 percent of funds allocated to the State were used to assist locals and implement the programs. We purchase licensing and advertise it to our target audience of counties, municipalities, and local special service districts. We track interest and eligibility through an interest submission form. We then organize those responses according to need and engage with those entities. We track each onboarding and implementation and their progress in a separate software program, as well as the distribution of the licensing and costs of those services, backed up by the data in the software platforms to ensure that we are meeting the 80 percent to locals and 25 percent to rural communities. We constantly check those numbers to ensure we hit the required target percentages.

Question 4. What challenges do States face in implementing SLCGP funds?

Answer. One of the biggest challenges is the continuity of funds. The cybersecurity risk is prevalent and communities are undermanned and underfunded for the fight against cyber attacks. The grants help kickstart programs, but without continued funds it will be hard to sustain programs or expand into other needed areas of cybersecurity protection. In some cases locals see that the funds are only for a limited time, which can cause hesitation in adoption because they know those programs could cease, leaving them trying to fill a gap they don't have the resources to fill.

Through funds allocated by the Utah Legislature, the State of Utah funded the entirety of the required match funds. Had that not been the case, it would have presented a challenge to local entities participating in the program, as they did not have the funds to meet the match requirements.

With the first round of funding, the State pursued a whole-of-State model and provided services to the local entities. At the same time, we carved out some funds to award directly to small or a handful of local entities as sub-recipients for their own cybersecurity projects. We found the sub-recipient process to be quite challenging from the standpoint of ensuring compliance with the SLCGP standards and funding quality projects. Though projects that met the SLCGP standards were implemented, we found that the quality of the implemented programs and funding did not go as far and was not as impactful on the overall need and the State cybersecurity risk that exists. In the end, we were able to stretch funds more efficiently and effectively and create more impact by purchasing and saving at the State level and providing those services to local entities.

Another big challenge is simply communicating and building trust with all eligible entities and ensuring they know the programs, what they are, and why they need them.

Question 5. The SLCGP's statutory authorization permits the Secretary of the Department of Homeland Security (DHS) to take action to ensure compliance. How has DHS—or CISA and the Federal Emergency Management Agency (FEMA)—ensured compliance with the grant program's requirements?

Answer. Initially, they have ensured compliance with the cybersecurity plan and its approval, in addition to submitting and approving projects and specific funds tied directly to those projects before releasing any funds. There is also the requirement locally for a cybersecurity commission, which helps CISA and FEMA tangentially with the compliance and proper use of the grant program. We must provide certain attestations and agreements to comply with certain requirements properly. After projects are started, they ensure compliance through our required quarterly financial reporting and yearly performance reporting on the progress of projects. These reports include narratives on progress, challenges, and proof of expenditures and use of funds in the previously-approved areas. They also do remote and site audits

and monitoring. The State of Utah had what CISA/FEMA called a Desk Review completed of our SLCGP program in May 2024. Personnel from DHS CISA and FEMA attended and asked various questions about the progress of our programs and were provided with evidence of progress.

Question 6. On average, how long does it take for a State or locality to start a cybersecurity program?

Answer. Depending on the methodology and implementation, it can take anywhere from 6 months to a year or more. Utah had a good process, which took around 6 months for the initial phase. We anticipated the SLCGP by hiring personnel, forming a Cybersecurity Commission, and then performing assessments to identify gaps. We coupled that with data from other State surveys and cybersecurity audits previously completed. We ensured consensus by reaching out to entities such as the League of Cities and Towns and the Association of Counties through presentations, visits, and various meetings. We built our plan and provided it to the Security Commission for approval. All of that took approximately 6 months. We then started an evaluation process of toolsets, using subsets of local governments as testers of the software and programs. We worked with the State legislature on needed bills and policy action during this process. Since we built it into our process from the beginning, it did not add significant time to the building of our cybersecurity program. Additional time could be added based on legislative cycles and the need for legislation. Adding all of this to our initial time frame of assessments and relationship building, it took 9 months for the program to be fully operational.

Because of the great community and already-established avenues of trust, we feel that Utah was able to move steadily and more quickly than perhaps some might be able to in establishing their programs. The centralized oversight provided by the SLCGP to the State helped speed up the creation and successful implementation of the cybersecurity program. There are many variables that could significantly increase or decrease the time it takes to implement a successful program, such as the support mechanisms and budget, additional personnel, travel, engagement time, and security awareness.

Question 7. If funding for this program is not reauthorized, are there Federal- or State-level funding alternatives you can pursue? If so, what are they and how do they compare with the SLCGP?

Answer. The State of Utah pursued and received all of the needed match funds for this program from the State legislature. We are currently pursuing State-level consensus for continued funding, anticipating the possible conclusion of the SLCGP program. We have not yet received permanent funding, but we continue to work the State legislature to help understand the need. We anticipate the State legislature will consider additional funding during the next legislative session in January 2026. Beyond this, there are no other alternatives that exist for appropriately funding these cybersecurity programs. At the local level, they have been unable to adequately find and fund proper cybersecurity, both from the standpoint of tool sets and trained personnel.

Even with the success or failure of receiving funding at a State level for the programs created through the SLCGP program, the cybersecurity risk is still present and more significant than what we can cover with SLCGP funds or State dollars alone. We do not currently cover all possible government entities with our programs, such as K–12 schools. We are providing only a small sliver of the possible baseline security needs that exist to protect an entity properly. We are hoping for a combination of both to maintain current programs and expand in other areas of security need.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR KEVIN KRAMER

Question 1. Are you aware of any instances in which the State and Local Cybersecurity Grant Program (SLCGP) has not been fully utilized in a given fiscal year? If so, how can we eliminate waste?

Answer. The National League of Cities is not aware of specific instances of underutilization by participants in the SLCGP. Generally speaking, NLC believes that one key way to improve the efficiency of SLCGP would be to reduce the number of intermediaries needed to manage each dollar. For that reason, NLC urges Congress to include a direct grant fund within the reauthorization of SLCGP, to allow larger jurisdictions such as Louisville Metro Government to directly apply for, access, and manage a direct Federal grant.

Question 2. What challenges do States face in implementing SLCGP funds?

Answer. The biggest challenge in implementing SLCGP for localities has been any delay or unpredictability in releasing SLCGP funds to States and the resulting compressions in State application time lines. Short application windows are challenging

for smaller jurisdictions to manage, and a lack of predictability in funding availability between fiscal years, as well as the program's titration of match requirements, makes the program more difficult to participate in and less appealing to potential grantees. Creating a consistent match requirement across grant years will help to alleviate some of this uncertainty. In Louisville Metro Government, while our staff were familiar with State and Federal grants, it still took several weeks to ensure compliance with internal processes for coding and disbursing funds.

Question 3. The SLCGP's statutory authorization permits the Secretary of the Department of Homeland Security (DHS) to take action to ensure compliance. How has DHS—or the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA)—ensured compliance with the grant program's requirements?

Answer. DHS, via CISA and FEMA, require grantees to provide quarterly reports on progress, as well as annual participation in the nationwide Cybersecurity Review (NCSR) assessment process. Participation in NCSR is open to all State, local, Tribal, and territorial entities on a free, voluntary basis through the Center for Internet Security, and is mandatory for recipients of Homeland Security Grant Program and SLCGP funds. NCSR is based on the NIST Cybersecurity Framework and is intended to assess program maturity. Use of the NCSR can help localities identify gaps, benchmark progress, assess program performance, and provides valuable information to the larger government cybersecurity community about needs and overall preparedness.

Question 4. On average, how long does it take for a State or locality to start a cybersecurity program?

Answer. Depending on what elements are being considered, it could take a local government a year to several years to stand up meaningful, well-planned cyber defenses. Local cybersecurity is an evolving target, even for well-resourced jurisdictions. For a smaller entity with an IT department but no dedicated full time cybersecurity staff, this process might look like conducting initial assessments against metrics such as the NIST Cybersecurity Framework or the National Cybersecurity Review, procuring network monitoring and other services from a vendor, and addressing any major low-hanging targets, such as switching the jurisdiction to the .gov domain, creating an incident response plan, implementing across-the-board two-factor authentication, moving to the cloud, establishing regular network backups, or other actions. Implementation of several of any combination of the above, when accounting for planning, procurement, and implementation, which impact many city departments, could easily take multiple years.

For a single, relatively simple grant-funded objective, such as implementation of email filtering or antivirus protection for municipal networks, individual jurisdictions may be able to accomplish that goal within a couple of years, depending on the alignment of Federal funding cycles, local fiscal years, calendar years, and procurement processes, as well as demands on internal staff capacity.

Question 5. If funding for this program is not reauthorized, are there Federal- or State-level funding alternatives you can pursue? If so, what are they and how do they compare with the SLCGP?

Answer. There are no direct replacements at the State or Federal level for SLCGP. At the Federal level, while other homeland security grant programs allow for some use for cybersecurity, there is no comparable grant program dedicated to State and local cybersecurity capacity. Local governments benefit from a dedicated funding stream for cybersecurity needs. State and local governments have also benefited from the framework SLCGP has created for more holistic intergovernmental coordination on cybersecurity. A fragmented approach to funding across multiple other grant programs, in addition to not replacing the actual resources provided by SLCGP, would not provide this supportive framework to the local cybersecurity effort. SLCGP is uniquely tailored to address the needs of rural communities in particular, and smaller and rural jurisdictions would be disproportionately affected by the loss of SLCGP.

Question 6. Do you share cybersecurity best practices and/or services with surrounding communities? If so, please explain how you do this.

Answer. Louisville Metro Government shares both cybersecurity best practices and services with other jurisdictions throughout the Commonwealth of Kentucky. LMG participates in a number of State and regional working groups focused on cybersecurity. LMG staff also present educational material to local government-focused groups such as the Kentucky Association of Counties and the Jefferson County League of Cities, which helps us provide support to smaller jurisdictions. Louisville Metro Government also provides pro bono services directly to smaller municipalities in the region.

As part of LMG's SLCGP grant expenditure, we are establishing the Kentucky Cyber Threat Intelligence Cooperative (KCTIC). Through this effort, we are addressing 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 and we anticipate this project having benefits for communities throughout the region and the Commonwealth.

The testimony by all witnesses during the April 1 hearing supports timely reauthorization of the State and Local Government Cybersecurity Grant Program. The National League of Cities thanks the subcommittee for its consideration and for the opportunity to respond to its questions for the record.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR MARK RAYMOND

Question 1. In reviewing your Cybersecurity Plan, did the Cybersecurity and Infrastructure Security Agency (CISA) help ensure your plan was implementable and reflective of the needs of your State? Please explain.

Answer. Yes, our CISA representative was a foundational resource for the State's efforts in developing and reviewing our Cyber Plan. Connecticut formed a multi-stakeholder committee to perform overall cybersecurity review. Our Cybersecurity Advisor, David Palmbach, participated in that committee. Through David, CISA provided insight into what threats were happening nationally and how our State compared to those threats. CISA provided context about what other States and local governments were experiencing related to cyber responses and organization structures. Finally, CISA ensured that all the capabilities of CISA and MS–ISAC are being utilized appropriately within the Cybersecurity Plan. This included items such as cyber-hygiene, DOT GOV implementation services, on-going vulnerability scanning and education services such as table-top exercises.

Question 2. Are you aware of any instances in which the State and Local Cybersecurity Grant Program (SLCGP) has not been fully utilized in a given fiscal year? If so, how can we eliminate waste?

Answer. We are not aware of any instances where the SLCGP funds have not been fully utilized. Since each award year of the grant program has a 4-year period of performance, we do not expect to see this in the future. Looking forward, availability of match funding will continue to be a struggle for governments; however, the 4-year period creates several options in which to arrange for match funds and successfully utilize all grant awards.

In 2022, which was the first offering of the program in Connecticut, we received 100 applications (97 from local entities) totaling over $13.7 million ($12.3 Federal share) of which we only had $2.9 million ($2.6 Federal) to subgrant. The rural share of this totaled over $7 million. We ended up prioritizing projects based on recommendations from the chartered planning subcommittee, and subgranted to 45 entities. We expect the 2023 round to be the same which shows the importance of the grants to our entities.

Question 3. Can you please describe how you track funding to ensure that the SLCGP's allocation requirements for local and rural entities are met?

Answer. Through our sub-application process and data collection, we ask entities to identify if they are rural (based on the Federal grant definition). Using the fiscal year 2022 funds, we subgranted $2,071,243 to rural entities.

Question 4. What challenges do States face in implementing SLCGP funds?

Answer. One common refrain is the changing match rates across the life of the grant. As each yearly award has a multi-year period of performance, the State granting agency and many subgrantees will face the complexity of managing different fiscal formulas for the same program.

Additionally, rising technology costs for equipment can diminish the overall effectiveness of any individual grant. This will be particularly acute in the last 2 years of the program as the funds identified for the grant are projected to be drop lower than Year 2 funds.

In resource-constrained environments, emerging threats often drive a rearrangement of priorities. State and local governments are expected to be under additional fiscal stress in cyber as greater responsibility is being passed to the State level.

Operationally, the State has only identified minor challenges to implementing the grant program. There was a delay in opening the sub-application period due to the

need to have a CISA-approved Cybersecurity Plan, but the 4-year period of performance allows ample time for awarded entities to complete projects.

Question 5. The SLCGP's statutory authorization permits the Secretary of the Department of Homeland Security (DHS) to take action to ensure compliance. How has DHS—or CISA and the Federal Emergency Management Agency (FEMA)—ensured compliance with the grant program's requirements?

Answer. FEMA/CISA provide extensive guidance through the notice of funding opportunity, technical assistance, and webinars and grant support. The assigned SLCGP program officer from FEMA has been a great resource for grant eligibility and guidance. Additionally, Connecticut participated in a monitoring visit from SLCGP staff for compliance and to explain the State's implementation process.

Question 6. On average, how long does it take for a State or locality to start a cybersecurity program?

Answer. Launching a cybersecurity program generally involves assessment, planning, procurement, staffing, implementation and maintenance phases, and generally, with steady resourcing and funding it takes 3–5 years as an iterative, consistent effort for a large entity to establish program fundamentals. For localities with limited staff, the process can stretch longer or proceed in smaller steps. In theory a smaller municipality could implement the basics but in practice many small municipalities lack the manpower, expertise, and continuity of personnel, funding, and experience to focus on cybersecurity full-time.

Progress at the municipal level has been incremental. Since 2023, Connecticut localities & school districts have been taking advantage of a free municipal cyber assessment program as planning groundwork in risk identification and improvement plans. Connecticut is using these plans to create a "menu" of cybersecurity projects & areas of focus for towns and to prioritize SLCGP funding efforts.

With the continued infusion of Federal funds and State of Connecticut coordination, the hope is that even the smallest municipalities will have at least a baseline cybersecurity framework in place within a few years. The on-going audits and assessments will continue to highlight gaps, but they also show that progress is being made—on a realistic, phased time line—toward standardized cyber defenses across Connecticut's State, city, and town governments.

Equally important to starting a cyber program is the need to both sustain and advance these programs. While we have imperfect views of what lies ahead, most professionals in this area expect the maturation of artificial intelligence to greatly increase the capabilities of cybersecurity threat actors. State and local governments must continue to address overall risk reductions in the face of sophisticated and ever-evolving threats and adversaries.

Question 7. If funding for this program is not reauthorized, are there Federal- or State-level funding alternatives you can pursue? If so, what are they and how do they compare with the SLCGP?

Answer. State and local government budgets remain under pressure from rising costs that push up against Constitutional spending caps and balanced budget requirements. These pressures could intensify if Congress enacts changes to mandatory programs that increase the State's share of funding beyond current levels.

Connecticut does not have a dedicated source of funding for cybersecurity initiatives that could be used to replace this program. Cybersecurity is an eligible expense under the FEMA Homeland Security Grant Program (HSGP) and Connecticut has leveraged that program for vital cybersecurity training and assessment programs to local entities. If SLCGP was cut, and HSGP also, that would leave a gap in providing funding support to local entities. HSGP funds have been used for cybersecurity training personnel, subgrants to local jurisdictions for cybersecurity training, and fully funded cybersecurity risk assessments. Revisiting that source may provide a modest amount to make incremental improvement. This would not be a substantive way to reduce State and local cyber risk.

One suggestion that might help sustain cybersecurity improvements would be to include State-wide cybersecurity as a cost that did not require cost allocation under the larger Federal programs (Medicaid, Income Security, Transportation, Education). Cost allocation of cybersecurity costs represents a complicated limitation on the whole-of-government cyber approach. The ability to use a small percentage of the existing funds that flow to States as a mechanism to improve cybersecurity outcomes on a systemic basis may allow States to fill critical gaps at the State and local government level.

○