State of Utah

SPENCER J. COX
Governor

DEIDRE M. HENDERSON
Lieutenant Governor

Department of Government Operations
Division of Technology Services

MARVIN DODGE
Executive Director

ALAN FULLER
Chief Information Officer

Alan Fuller
Chief Information Officer
Division of Technology Services, State of Utah
NASCIO Secretary-Treasurer

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

April 1, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee:

I am Alan Fuller, Chief Information Officer for the State of Utah, a role to which I was appointed by Governor Cox in March of 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 statewide 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	4.18	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	1.2	1.2	1.7	1.6	3.2	2.6	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	1.9	2.3	1.6	3.0	3.3	2.3
	PR.DS	Data Security	3.74	2.8	1.5	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	2.0	1.8	2.4	2.6	1.4	1.6	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	2.1	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	2.42	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 statewide 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 two of these.

Shortly before Christmas, the CIO of a local airport urgently contacted me about a cyberattack. 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 911 dispatch center in Utah was the victim of a ransomware attack on systems that provide 911 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, healthcare 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 two 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% 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 statewide 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 stakeholders 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.

Robert Huber
Chief Security Officer, Head of Research and President of Tenable Public Sector, Tenable, Inc.
House Homeland Security Committee
Subcommittee on Cybersecurity and Infrastructure Protection
"Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program"
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 startups 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

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

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 cyberattack on the Littleton Electric Light and Water Departments (LELWD) in Massachusetts, the 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 U.S. 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

---

[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.

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 U.S. effectively detect, mitigate, and recover from these cyberattacks, 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 cyberattacks targeting state and local government organizations during the first eight months of 2023 compared to the same period in 2022.[8] Malware attacks surged by 148% and CIS' Review also found ransomware incidents on the rise, climbing by 51% during this time period. Non-malware attacks grew by 37%, 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% rise in endpoint security service incidents, suggesting a significant uptick in breaches and unauthorized access attempts.[10] These findings further underline the 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 cyberattacks.[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]

---

[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.

[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.

State and Local Cybersecurity Grant Program

Given the ongoing 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 four 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% of eligible localities statewide 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.

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, statewide 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 intelligence 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 cyberattack 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% 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 cyberattacks.

[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.

Benefits of Whole-of-State Approach to Cybersecurity

A whole-of-state approach fosters statewide 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 statewide 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 statewide. These requirements promote addressing risks proactively while providing a clear roadmap for enhancing resilience against cybersecurity threats.

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 four-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% in FY 2022 to 40% by FY 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, 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 two-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

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

[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/.

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.

NATIONAL LEAGUE OF CITIES

A CENTURY OF STRENGTHENING CITIES

STATEMENT OF

THE HONORABLE KEVIN KRAMER

FIRST VICE PRESIDENT, NATIONAL LEAGUE OF CITIES AND

COUNCILMAN, LOUISVILLE METROPOLITAN GOVERNMENT, KENTUCKY

ON BEHALF OF THE NATIONAL LEAGUE OF CITIES

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

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

APRIL 1, 2025

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

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

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

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

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

Louisville Metro Government's Perspective

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

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

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

Reauthorizing the State and Local Cybersecurity Grant Program

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

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

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

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

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

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

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

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

April 1, 2025

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

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

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

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

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

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

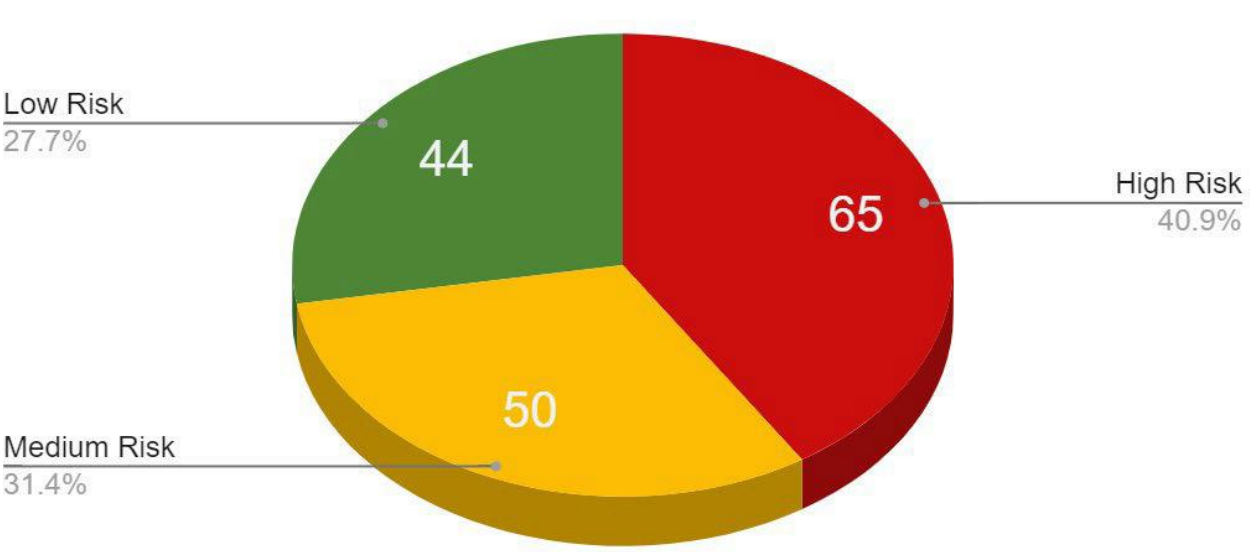
To that end, through the grant, we have expanded state offerings to local governments, including risk assessments, dot gov domain expansion, multi-factor authentication, ransomware prevention software, employee training, and other critical services. Perhaps most important, however, is the spirit of trust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

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

Connecticut Experience

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

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



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

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

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

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

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

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

Next Steps

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

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

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

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