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.