ALLIANCE FOR DIGITAL INNOVATION BETTER IDENTITY COALITION ITI

Cybersecurity Coalition TECHNET THE VOICE OF THE INNOVATION ECONOMY

September 2, 2025

The Honorable Susan Collins
Chair, Appropriations Committee
United States Senate
413 Dirksen Senate Office Building

The Honorable Patty Murray
Vice Chair, Appropriations Committee
United States Senate
154 Russell Senate Office Building

The Honorable Tom Cole
Chair, Appropriations Committee
United House of Representatives
2207 Rayburn House Office Building

The Honorable Rosa DeLauro
Ranking Member, Appropriations Committee
United House of Representatives
2413 Rayburn House Office Building

The Honorable Rand Paul
Chair, Homeland Security and Governmental
Affairs Committee
295 Russell Senate Office Building

The Honorable Gary Peters
Ranking Member, Homeland Security and
Governmental Affairs Committee
724 Hart Senate Office Building

The Honorable Andrew Garbarino
Chair, Homeland Security Committee
United House of Representatives
2344 Rayburn House Office Building

The Honorable Bennie Thompson
Ranking Member, Homeland Security Committee
United House of Representatives
2466 Rayburn House Office Building

Re: Support for Reauthorization of the State and Local Cybersecurity Grant Program

Dear Chair Collins, Vice Chair Murray, Chairman Cole, Ranking Member DeLauro, Chairman Paul, Ranking Member Peters, Chairman Garbarino, and Ranking Member Thompson:

We, the undersigned associations, are writing to strongly support the continued funding of the State and Local Cybersecurity Grant Program (SLCGP) (the Grant Program).

Cybersecurity threats are an escalating risk that demands immediate and sustained action to prevent serious harm to American communities. Nation-state actors are persistently targeting U.S. critical infrastructure and systems at the state, local, tribal, and territorial (SLTT) government levels, seeking to conduct espionage, disrupt essential services, and erode public trust. Recent trends highlight the severity of this threat. According to CrowdStrike's 2025 Global Threat Report, malicious cyber activity linked to the People's Republic of China surged by 150 percent overall in 2024, with some targeted industries suffering 200 percent to 300 percent more attacks than the previous year. The Federal Bureau of Investigation (FBI), in its Internet Crime Report 2024, highlighted $16.6 billion in losses reported to the Internet Crime Complaint Center (IC3) over the past year. Actors affiliated with Russia, North Korea, and Iran remain persistent, sophisticated, and motivated.

Groups affiliated with the People's Republic of China are conducting unauthorized access to U.S. infrastructure, and one of these groups, Volt Typhoon, has already prepositioned itself within our networks. This poses one of the most urgent national security threats facing our country today. Volt Typhoon focuses on gaining long-term, covert access to critical infrastructure systems—including energy, transportation, and water sectors—using legitimate administrative tools to avoid detection. These coordinated campaigns demonstrate how nation-state actors deliberately target U.S. systems to influence decision-making during a crisis and to advance their geopolitical goals through cyber operations. Importantly, while much of our Nation's critical infrastructure is owned and operated by state and local governments, its cyber defense is not just a local issue. It is a vital component of national security because the Department of Defense relies on this civilian-operated infrastructure for military readiness and power projection, making state, local, tribal, and territorial cybersecurity a foundational element of our national defense posture.

The potential consequences of such attacks can be severe: loss of access to power, water, health care, and transportation; interruption of small and large business operations; suspension of government services and military operations; and lasting damage to economic productivity and resilience. These impacts are not hypothetical—they are happening. A sample of recent incidents include:

- **U.S. Military Readiness:** Chinese state-sponsored actors infiltrated critical infrastructure in Guam, including communications and utilities supporting U.S. military bases. The attackers pre-positioned malware capable of disrupting communications between the U.S. and Asia during a potential crisis, demonstrating a direct threat to military readiness.
- **Water Sector:** An Iranian-affiliated group hacked the Municipal Water Authority of Aliquippa, PA, by targeting an Israeli-made device, forcing the utility to switch to manual controls. In another example, an attacker breached the computer system in the Oldsmar, FL, water treatment plant and attempted to poison the water supply for 15,000 residents by increasing sodium hydroxide levels to a dangerous amount. These, along with other breaches at U.S. water utilities, confirms that foreign actors are actively targeting SLTT-owned water infrastructure, which could impact public health and safety.
- **Transportation Sector:** Ransomware attacks on multiple transit systems in Pennsylvania disrupted rail tracking, public announcement systems, and real-time schedules, causing significant delays for commuters and impacting regional commerce.
- **Municipal Governments:** Attacks on cities like Wichita, KS, Oakland, CA, and Columbus, OH, forced agencies offline, disrupted services like water bill payments and 911 administrative lines, and resulted in the leak of sensitive city data. In some of these incidents financial data of residents was compromised, and sensitive personal information of city employees, including police officers and firefighters, was exposed.
- **Electric Grid Sector:** In the past four years, 16 Cyber Security Incident reports were submitted to the sector's designated cybersecurity and threat intelligence hub, representing attempted system compromises. These incidents originated from different regional entities and included failed login attempts and network scanning, primarily from foreign IP addresses. And more locally, the Littleton Electric Light & Water Department in Massachusetts discovered hackers connected to the Volt Typhoon campaign spent nearly one year inside the systems of their major utility company.
- **Health Care Sector:** The breach at Change Healthcare caused major operational and financial disruption for hospitals nationwide. A survey found that 94 percent of hospitals suffered financial losses, and 74 percent reported direct impacts on patient care delivery.
- **Judicial Systems:** Attacks on the court systems in Fulton County, GA, and the entire state of Kansas took IT systems offline for weeks. This slowed court proceedings delayed police reporting and posed significant risks to public safety and the rule of law.
- **Public Safety:** The Office of the Attorney General of Virginia was crippled by a cyberattack, which caused nearly all technology systems to be taken offline and significantly slowed the provision of legal services due to suspicious activity.
- **K-12 Education:** The Los Angeles Unified School District was hit by a ransomware attack where the attackers leaked 500 GB of highly sensitive student and employee data, including psychological records and Social Security numbers.
- **Tribal Governments:** A ransomware attack on the Sault Ste. Marie Tribe of Chippewa Indians shut down government offices, health care clinics, casinos, and gas stations, demonstrating that tribal entities face the same crippling threats.

To defend against these real and present threats, a comprehensive and coordinated approach to cybersecurity risk management is essential, grounded in proven standards and best practices. The Department of Homeland Security's (DHS) SLCGP was created to do exactly that. The Grant Program is the only federal program dedicated exclusively to helping states, local governments, and rural areas address cybersecurity risks and protect their critical infrastructure. Funded at $1 billion over four years, it supports the development of statewide cyber strategies, completion of risk assessments, and implementation of threat mitigation. To access funds, states must follow a structured process beginning with the establishment of a Cybersecurity Planning Committee. The Committee must include representatives from across state and local organizations and is responsible for developing a statewide cybersecurity plan. These plans must reflect recognized cybersecurity best practices and standards, incorporate local government activity, define measurable progress metrics, and summarize associated projects. States are also required to conduct capability assessments, evaluate their current cybersecurity posture, and meet federal cost-share requirements. DHS releases the funding to the states after ensuring the cyber plans and associated projects align with the program's requirements.

This rigorous structure has driven meaningful results and fostered long-term strategic planning. For example, in Texas grant funds were used to modernize safeguards and advance incident response capabilities, and in Louisiana municipal agencies adopted standardized incident response protocols and deployed new security devices. In New York, the whole-of-state approach was advanced through threat detection and multi-factor authentication deployments. States like New Hampshire, Virginia, and Maryland have conducted vulnerability assessments, while Michigan and Arizona have provided best-practice cyber solutions to identify, protect, detect, and respond to cyber incidents. Communities in Kentucky used funds to establish a cyber threat intelligence-sharing platform, enabling public and private sector partners to anonymously share near real-time threat information.

A recent report found that DHS's administration of the Grant Program met all statutory requirements, applied structured processes and checklists to ensure applicants met the law's criteria, and provided flexibility to help states comply. The Program has established a successful model for federal government participation in fulfilling its national security responsibility. This is only the beginning of the work that is necessary to protect our nation.

The Grant Program is currently set to expire on September 30, 2025. Without continued funding, hard-won progress will stall, and communities across the country will be left vulnerable—handing our adversaries a dangerous advantage. While non-federal governments must take on their requisite cybersecurity responsibilities, they cannot meet this challenge alone. The scale and urgency of this national security challenge require a coordinated national response, backed by sustained federal investment. Allowing the program to lapse would weaken domestic cyber resilience and give adversaries an opportunity to exploit known vulnerabilities at a time of rising geopolitical tension.

We support Congress's efforts to continue SLCGP and urge Congress to fund the Grant Program without delay. We recommend establishing a stable and predictable federal funding stream of $4.5 billion over two years, paired with a consistent state cost-share mechanism. The program should continue to promote the adoption of proven, measurable cybersecurity standards and support collaborative, strategic implementation across state, local, tribal, and territorial governments.

Determining the exact level of funding required to protect state and local systems from cyberattacks is difficult, but the necessary investment will be substantial. While the total cost is hard to quantify, the consequences of inaction are already clear. For example, North Korea has reportedly stolen more than $3 billion through just 58 cyberattacks, demonstrating the scale of the threat and the value hostile actors place on cyber operations.

Further, while cost comparisons are not always precise, they help underscore the scale of investment required. The U.S. Department of Defense spends more than $2 billion each day to defend our nation. Committing a fraction of that annual amount to secure critical systems across state and local governments would be a strategic and proportionate response. Taking action now would strengthen national resilience and reduce the risk of major disruptions before they occur.

These are practical and necessary steps to achieve measurable progress against a well-documented national security threat. Given the potential economic and operational damage from a major cyberattack on U.S. infrastructure, continued federal investment is both justified and urgent.

Our respective members stand ready to work with Congress to ensure that state and local governments have the tools and support they need to defend the systems that millions of Americans rely on every day. This is not only a prudent investment, but it is also a critical step toward protecting our economy, our infrastructure, and our national security.

Thank you for your leadership on this issue and for your continued commitment to securing the Nation's future.

Sincerely,

Alliance for Digital Innovation (ADI)

Better Identity Coalition (BIC)

Cybersecurity Coalition

Information Technology Industry Council (ITI)

TechNet