September 3, 2025

The Honorable Andrew Garbarino
Chairman, House Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

The Honorable Bennie Thompson
Ranking Member, House Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

The Honorable Rand Paul
Chairman, Senate Homeland Security and Governmental Affairs Committee
295 Russell Senate Office Building
Washington, DC 20510

The Honorable Gary Peters
Ranking Member, Senate Homeland Security and Governmental Affairs Committee
724 Hart Senate Office Building
Washington, DC 20510

The Honorable Chairman Eric Swalwell
Ranking Member, House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection
H2-176 Ford House Office Building
Washington, DC 20515

The Honorable Kristi Noem
Secretary of Homeland Security,
U.S. Department of Homeland Security,
Washington, DC 20528

Letter of Support for the State and Local Cybersecurity Grant Program (SLCGP)

Dear Chairman Garbarino, Ranking Member Thompson, Chairman Paul, Ranking Member Peters, Ranking Member Swalwell, and Secretary Noem,

On behalf of the Operational Technology Cybersecurity Coalition and other concerned cybersecurity organizations, we write to express our strong support for the continuation and enhancement of the State and Local Cybersecurity Grant Program (SLCGP). The OTCC works with industry and government stakeholders to enhance the resilience of our nation's critical infrastructure, recognizing that cybersecurity is a team sport in this era of accelerating threats.

The SLCGP represents a crucial piece of this multi-stakeholder approach which brings together federal, state, local, tribal, and territorial (SLTT) government efforts. These entities are at the forefront of defending critical infrastructure, public services, and other vital systems and assets from an increasing array of cyber threats, including sophisticated ransomware and nation-state attacks. Many SLTT entities, particularly smaller and rural jurisdictions, face significant challenges due to budget constraints and limited cybersecurity expertise. The SLCGP provides vital funding that helps bridge these gaps.

We are encouraged by the program's accomplishments since its establishment in 2021. By providing financial support and requiring strategic planning, the SLCGP lays a strong foundation for SLTT governments to improve their cybersecurity posture. The program's objectives to improve governance and planning, conduct assessments, implement mitigation measures, and support workforce development are essential steps in managing and reducing systemic cyber risks.

Furthermore, the SLCGP significantly advances the critical concept of a "whole-of-nation" approach to cybersecurity, fostering collaboration among state agencies, local governments, federal agencies, and private sector entities. It enables resource sharing, reduces redundancies, improves efficiency, and creates a unified defense strategy. This collaborative model aligns directly with our view that cybersecurity is a team sport and requires every organization that can contribute meaningful solutions to join the effort.

The flexibility for states to provide shared services to local governments is also a key benefit, allowing smaller communities to access vital technology services they otherwise could not afford. The program encourages the implementation of essential best practices, such as multi-factor authentication, enhanced logging, data encryption, and migrating to the .gov domain. We note that SLCGP projects, through a risk-informed approach like exposure management, can help SLTTs understand and secure their expanded environment, including critical infrastructure and operational technology (OT).

While the SLCGP has a proven track record of accomplishment, including specific examples of funded tools helping to block major cyber attack incidents, we believe its full potential can be further unlocked with key improvements. The uncertainty around the program's long-term future remains an impediment to success and discourages investment in multi-year projects. Providing long-term stability and assurance through a longer reauthorization is vital. Additionally, the increasing cost-share requirements pose significant challenges, particularly for rural areas and small jurisdictions. Establishing a lower and consistent match percentage would reduce financial strain and promote equitable access to funding. Simplifying the application process would also encourage participation from smaller communities with limited staff.

While we acknowledge that the obligation rate of the grant funding could be improved, we nevertheless believe that reauthorizing and enhancing the SLCGP is essential for empowering state and local preparedness and strengthening the resilience of critical infrastructure. As the threat landscape continues to evolve and attacks become more sophisticated, ensuring SLTT governments have the necessary resources and support is paramount to national security and the well-being of our communities.

We strongly encourage Congress to reauthorize and adequately and consistently fund the SLCGP. The program is a crucial piece of the national cybersecurity puzzle and helps build a solid foundation for strengthening defenses across all levels of government.

Thank you for your leadership in advancing cybersecurity and safeguarding our nation's critical infrastructure. We look forward to supporting efforts to reauthorize and improve this vital program.

Sincerely,

Association of the United States Cyber Forces (AUSCF)

CSC 2.0

Cyber Threat Alliance (CTA)

Global Cyber Alliance (GCA)

Information Technology Industry Council (ITI)

Operational Technology Cybersecurity Coalition (OTCC)

Software & Information Industry Association (SIIA)

Strategic Cybersecurity Coalition (SCC)

McCrary Institute for Cyber and Critical Infrastructure Security