COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program

April 1, 2025

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

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

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

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

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

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

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

The relationships built through this process have facilitated new, strategic state-wide collaborations.

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

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

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

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

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

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

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

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

Congress would never leave state and local governments to fend for themselves in a physical attack. We cannot leave them to fend for themselves in cyberspace.

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

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

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

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

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

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

# # #

Media contact