



# COMMITTEE ON HOMELAND SECURITY

*Ranking Member Bennie G. Thompson*

**FOR IMMEDIATE RELEASE**

## **Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)**

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

**April 1, 2025**

Establishing this program four years ago was the product of bipartisan legislation developed by this subcommittee, demonstrating how members can come together to develop a solution that makes a meaningful difference in addressing a serious cybersecurity problem.

That kind of bipartisan work is just as necessary today, and I am confident today's hearing will help inform this subcommittee's efforts to extend necessary support to state and local governments.

As we consider State and local cyber grant reauthorization, it is important to remember that cyber attacks on state and local governments affect all our districts, whether they are in blue states or red states and whether they are urban, suburban, or rural.

In my district, the City of Hayward suffered a ransomware attack in the summer of 2023 that shut down the city's computer networks for more than two weeks.

And just two months ago, Hayward began notifying individuals that personally identifiable information, including social security numbers and sensitive medical information, had been breached as part of that ransomware incident.

I know this story is not unusual, and I am sure my colleagues have also heard from local governments impacted by cyber attacks and looking for help.

With cyber attacks coming from foreign criminal gangs and nation-state adversaries, we cannot leave our state and local governments to fend for themselves.

Federal support for state and local governments is necessary to address this national security threat, and the State and Local Cybersecurity Grant Program reflects that understanding.

By providing \$1 billion to state, local, tribal and territorial governments, Congress took a major step in strengthening cyber defenses and bringing stakeholders together to develop and implement much-needed cybersecurity planning by state governments.

We are a more secure country today because of this investment.

But as we all know, our adversaries are not stopping their efforts to breach public sector networks.

When the State and Local Cyber Grant Program was created, our primary concern was the ransomware epidemic plaguing our communities.

Of course, that threat remains, but China's campaign to pre-position on our critical infrastructure networks for potential future destructive attacks is even more alarming.

While much of our critical infrastructure is privately owned, some of our most vital services are provided by the public sector.

Publicly owned and operated water and electric utilities, transportation systems, and emergency services could all be targets in destructive attacks by China or other adversaries.

Reauthorizing the cybersecurity grant program is necessary to ensure we do not take our foot off the gas at this critical time, and passing a reauthorization bill before the program expires in September is one of my top priorities this year.

What I have heard from stakeholders is appreciation for the tremendous value of this program and a desire for sustained, predictable, and consistent funding levels that will allow state and local governments to build on their progress and properly budget and plan their efforts.

The cybersecurity grant program operates under a partnership between FEMA and CISA, two incredibly important agencies that have unfortunately come under attack in recent months.

By leveraging FEMA's grants administration expertise and CISA's cybersecurity expertise, this program has been able to deliver for state and local governments in ways that would be impossible without that partnership.

Trump Administration plans to eliminate FEMA and further cut CISA's workforce would devastate DHS's ability to support state and local governments across a range of threats, including cyber attacks.

The cybersecurity grant program demonstrates the value of collaboration between DHS's components, and I hope we can work in a bipartisan way to better educate Secretary Noem about the tremendous value these agencies provide the American public.

Additionally, I am deeply concerned by reports that FEMA has been pausing distributions of funding to implement cyber grants, along with other grant programs.

China is not pausing their efforts to target our critical infrastructure. We should not pause our efforts to defend ourselves.

I urge the Trump Administration to release cyber grant funds to states, territories, and tribes and to comply with court orders against its illegal pauses.

Finally, I would like to thank the witnesses for appearing before us today.

Expertise from both the public and private sector is invaluable as we look to reauthorize and improve the State and Local Cybersecurity Grant Program, and I look forward to their testimony.

# # #

[Media contact](#)