COMMITTEE ON HOMELAND SECURITY

The "State and Local Cybersecurity Improvement Act"

As Introduced by Rep. Clarke (D-NY), Rep. Garbarino (R-NY), Ranking Member Katko (R-NY), Rep. Kilmer (D-WA), Rep. McCaul (R-TX), Rep. Ruppersberger (D-MD), and Chairman Thompson (D-MS)

The State and Local Cybersecurity Improvement Act would authorize a new Department of Homeland Security (DHS) grant program to address cybersecurity vulnerabilities on State and local government networks. State and local governments are rich targets for cyber adversaries and the frequency of attacks is accelerating.

In 2020, ransomware attacks crippled State and local agencies, including the New Mexico Public Regulation Commission, a county library system in California, and police departments in North Miami Beach, FL and Trenton, NJ, along with many other communities scattered across the country. Already, in 2021, ransomware attacks have forced a school district in Massachusetts to cancel its first day of in-person classes and have threatened the Washington, DC police department with the release of sensitive data. In recent years, cities from Albany to Atlanta have been impacted– to the tune of nearly $20 million, in some cases. The Federal government needs to redouble its efforts at partnering with State and local governments to build robust cybersecurity defenses. The *State and Local Cybersecurity Improvement Act* will improve the ability of State and local governments to detect and defend against cyber-attacks by authorizing dedicated resources and support.

The State and Local Cybersecurity Improvement Act:

- Establishes a $500 million DHS grant program with a graduating cost-share that incentivizes States to increase funding for cybersecurity in their budgets;

- Requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop a Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments to, among other things, identify Federal resources that could be made available to State and local governments for cybersecurity purposes and set baseline objectives for State and local cybersecurity efforts;

- Requires State, Tribal, and territorial governments to develop comprehensive Cybersecurity Plans to guide the guide use of grant dollars;

- Establishes a State and Local Cybersecurity Resiliency Committee comprised representatives from State, local, Tribal, and territorial governments to advise and provide situational awareness to CISA regarding the cybersecurity needs of State, local, Tribal, and territorial governments; and

- Requires CISA to assess the feasibility of implementing a short-term rotational program for the detail of approved State, local, Tribal, and territorial government employees in cyber workforce positions at CISA.

Today, State and local governments are not in the position to defend their networks against the cyberattacks from sophisticated foreign adversaries or cyber criminals. Stretched State and local budgets have not adequately funded cybersecurity. Despite the potential national security consequences of a cyberattack against a State or local government, the Federal government has been slow to act. Passage of ***the State and Local Cybersecurity Improvement Act*** is an important first step toward defending State and local networks.

The State and Local Cybersecurity Improvement Act requires both the Federal government and its State partners to develop strategies to bolster State and local cybersecurity capabilities and provides funding to ensure those strategies are implemented. Investing in cybersecurity before a cyberattack saves money, protects important data housed on State and local networks, and ensures State and local governments can continue to provide the important services Americans rely on. A similar version of this bill passed the House by voice vote in the 116th Congress.