**Opening Statement as Prepared for Delivery by Chair Maggie Hassan**
**Emerging Threats and Spending Oversight Subcommittee Hearing**
**"Addressing Emerging Cybersecurity Threats to State and Local Government"**
**June 17, 2021**

Good morning. The Subcommittee on Emerging Threats and Spending Oversight convened today's hearing to discuss the threats to state and local entities from cyberattacks and the consequences of those attacks on national security, the economy, and the lives of our citizens. We will discuss what state and local entities need to be able to effectively respond to cyber threats, and how the federal government can best support state and local authorities as they work to combat the growing wave of cyberattacks.

While the SolarWinds, Colonial Pipeline, and JBS meatpacking cyberattacks rightly received a lot of attention in recent months, state, local, and tribal entities have also faced serious cyberattacks that can cripple services for citizens and decimate local budgets. The cybersecurity firm Emsisoft estimated that the total cost of publicly known ransomware attacks on state and local governments in 2020, including costs to restore functionality and services, was nearly one billion dollars. A report from cybersecurity firm Blue Voyant found that there was a 50 percent increase in the number of cyberattacks against state and local entities from 2017 to 2019. At the same time, the average ransom demanded in those attacks increased 10 times, and the average cost to taxpayers to clean up after a single cyberattack rose to the millions of dollars.

Today's hearing sheds a light on the impact of attacks like the one we saw on Sunapee School District in my home state of New Hampshire, which is represented today by Superintendent Russ Holden. Luckily for the Sunapee community, the district had a plan in place, including a separate backup system, so it was able to resume operations soon after the attack was discovered, without paying the ransom. Thank you, Superintendent Holden, for your leadership on cybersecurity for school districts.

Amid the COVID-19 pandemic, we have seen more than ever the importance of shoring up cybersecurity. State and local agencies depend on digital delivery of services to Americans, and many state and local employees are also connecting to central networks from home in order to do their work remotely.

More investment, at all levels of government, is needed to strengthen cyber defenses. A 2020 survey of state Chief Information Security Officers found that most states only spend 1 to 3 percent of their overall IT budgets on cybersecurity, compared to about 16 percent for federal agencies. And many local governments, with their smaller budgets, are even worse off.

Cybersecurity risks will continue to rise if state and local entities aren't able to strengthen their cyber resilience. I am working across the aisle to help state and local officials address cyber threats, and increase information sharing at the federal, state, and local level.

I am pleased that the most recent National Defense Authorization Act included my provision to provide each state with a federally funded cybersecurity coordinator. These coordinators will

provide each state – and the local governments within them – with a local contact who can provide support and technical knowledge, and act as a bridge to the federal government. I was very happy to recently learn that New Hampshire's coordinator came on board in the last week. In addition, this Congress, I introduced a bipartisan bill with Senator Cornyn to better enable the National Guard to support state and local government cybersecurity.

But we need to do more. That is why I am also working with my fellow Senators to craft a dedicated cybersecurity grant program for state and local governments.

I am excited to discuss these ideas and more with our five insightful witnesses today. Four of them represent a state, a county, a city, and a school district, and can help us better understand the unique environment that each have to operate within. They can also help us better understand which types of federal support may be the most effective. The fifth witness is an expert in federal cybersecurity policy and notably, a former senior staffer for the Homeland Security and Governmental Affairs Committee.

To all of our witnesses, I appreciate your willingness to testify, and I want to thank you all for the role you play in helping to keep us safe. I look forward to learning from you today.