Senator Rand Paul
Opening Statement
Hearing of the Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security & Governmental Affairs
"Addressing Emerging Cybersecurity Threats to State and Local Government"
June 17, 2021

Thank you Chairwoman Hassan, and thank you to our panelists today for your time. I look forward to hearing from each of you.

I'd like to begin my remarks with an observation, which is that the recent wave of ransomware attacks seems to have broken through into the public consciousness.

I traveled my home state of Kentucky extensively during the state work period earlier this month and was asked more questions about cybersecurity in those 10 days or so than in the previous 10 years.

Of course, we as policymakers have been concerned about malicious activity in cyberspace for some time now. In fact, at the Chairwoman's request, this subcommittee held a hearing on ransomware and cybersecurity this past December, and I'm grateful for her continued focus on this issue.

But from what I saw and heard from the people I represent, there's now a much more widespread appreciation for how disruptive these attacks can potentially be.

Obviously the Colonial Pipeline interruption and the specter of gas shortages was a major concern.

The Kentuckians I spoke to were also *very* concerned about the ransomware attack affecting North American meatpacking facilities owned by JBS, which may not have received quite as many headlines as the Colonial Pipeline incident, but which is every bit as alarming.

Clearly we have a problem on our hands. The nation must be able to secure its food supply and deliver fuel where it is needed. Recent cyberattacks have also targeted hospitals, school systems, water systems, and other essential services.

So how do we combat this?

As the old saying goes, an ounce of prevention is worth a pound of cure. Cybersecurity must be prioritized in the same way that any other essential services are prioritized.

As we will hear, recovering from cyber incidents such as ransomware attacks, and data breaches is several orders of magnitude more costly than what it takes to implement and maintain good cybersecurity practices on the front end.

Finally, I believe Congress needs to make sure that the federal government's role in detecting and responding to cyberattacks is limited and clearly defined, and that federal cybersecurity personnel are focused first and foremost on the security of federal information networks.

Senator Rand Paul
Opening Statement
Hearing of the Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security & Governmental Affairs
"Addressing Emerging Cybersecurity Threats to State and Local Government"
June 17, 2021

The government can and should share information on threats and best practices with the private sector and state, local, tribal and territorial authorities.

However, Congress must keep critical infrastructure operators and state, local, tribal and territorial governments in the proverbial "driver's seat" on cybersecurity.

I am particularly worried about a proposal that recently passed the House of Representatives, which would create a new multi-billion dollar grant program to subsidize state and local cybersecurity.

The Washington solution seems to be to throw money at every problem, with the result being a $28 trillion national debt.

As Americans, we face cybersecurity concerns that involve the availability of gasoline, and the food supply, and the electrical grid, water and sanitation systems, and our communications networks – indeed, some of the fundamental building blocks of our society.

I look forward to the conversation, and again, to the witnesses, thank you for your time.