Opening Statement of Chairman Rand Paul, M.D.
Subcommittee on Federal Spending Oversight & Emergency Management
"State and Local Cybersecurity: Defending Our Communities from Cyber Threats amid COVID-19"
December 2, 2020

I now call to order this hearing of the Senate Homeland Security and Governmental Affairs' Subcommittee on Federal Spending Oversight and Emergency Management.

The title of our discussion today is "State and Local Cybersecurity: Defending Our Communities from Cyber Threats amid COVID-19."

In preparing for this hearing, it's become clear to me that good cybersecurity practices require a near-constant struggle to stay ahead of events, and the real danger lies in getting complacent. Effective cybersecurity is an ongoing, everyday line of effort.

The threat landscape is diverse, the best practices are constantly changing, the information you get may not always be reliable, the maintenance tasks can seem overwhelming, and – most importantly – the stakes are high.

And in this context, I often found myself thinking: effective cybersecurity cannot move at quote "the speed of government."

By that I mean, cybersecurity as a 21st century public policy problem just is not "solvable" (or really even manageable) by 20th century government means. Regulation, mandates, and centralized action in general – these approaches are inadequate to match the pace of change that we have witnessed in the cybersecurity realm in recent years.

Congress needs to make sure that the government's role in detecting and responding to cyberattacks is clearly defined, and that they are focused first and foremost on the security of federal information networks. Today, we'll hear from the Department of Homeland Security about their cybersecurity work, how it is evolving, and about their approach to this complex range of threats.

With respect to individual actors in industries that are at the greatest risk of cyberattack—health care, education, financial services, retail, and critical infrastructure—the proliferation of

ransomware attacks over the past several months and years have made clear that these entities have to take on this responsibility themselves.

Irrespective of what the government is or is not doing, all cybersecurity is local, and so today we'll hear from experts in state government, the health care sector, and public education on their experiences with cyber incidents and the state of cybersecurity in these industries.

Fortunately, for both government and the private sector, the marketplace for cybersecurity services is continuing to grow and mature. We'll hear today from one such firm, Coveware Inc., that consults with private and public entities on cybersecurity and works with them to respond to cyber incidents.

I would like to thank Ranking Member Hassan for suggesting this hearing, and I look forward to hearing from our panelists.