Homeland Security and Governmental Affairs Committee
Federal Spending Oversight and Emergency Management Subcommittee

Ranking Member Margaret Wood Hassan
Opening Statement

Wednesday, December 2, 2020

Mr. Chairman, thank you for working with me to arrange this hearing. I deeply appreciate the opportunity to continue working on an issue that I believe is critical to our national security, as well as to the economic security of our nation. State and local governments have been prime targets for cyberattacks for a number of years. But the stakes have only grown as COVID-19 has forced millions of Americans to migrate their everyday activities to the online world. Many students now learn from their teachers on a computer instead of in the classroom. Doctors treat many patients through telemedicine instead of in-person. Governments handle many essential services online instead of at city hall. The massive increase in online activities over these past nine months means that the targets for cyber criminals have increased commensurately.

Unfortunately cyber criminals have taken advantage. One firm that tracks cyberattacks on schools and school districts reports that 44 attacks have occurred so far this school year, and many more likely went unreported. We will hear from the superintendent of one of those schools today. In the spring, INTERPOL warned that ransomware attacks against hospitals have grown significantly as hackers sensed an opportunity to extort more money in ransoms with hospitals overwhelmed with COVID patients.[1]

And about a month ago, a cyberattack hit the University of Vermont Medical Center, forcing it to divert patients to other facilities, thereby jeopardizing the care of many patients, especially those in nearby rural areas who do not have the resources to travel to the next closest hospital for treatment. The federal government has a responsibility to help protect our communities from these threats.

While the Cybersecurity and Infrastructure Security Agency has done a commendable job helping our state and local governments, the number and the severity of attacks on our communities continues to increase.

This hearing will help us identify ways for Congress and the federal government to better assist state and local governments in fending off these cyberattacks on our communities.

We have a great group of witnesses who can help us work through these challenges, including CISA Acting Director Brandon Wales, who we are happy to have here today.

[1] https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/#4e597bc558bc

With that said, we are missing our original federal witness—CISA Director Chris Krebs—because he was fired abruptly by the President two weeks ago.

Director Krebs led CISA in a non-partisan manner, and he approached his agency's most important task—securing the U.S. election infrastructure—with professionalism and tenacity. He was fired for doing his job and we are less safe because of it. It is imperative that we have strong, independent leadership at CISA going forward.

As the Biden Administration seeks to fill this position in 2021, I would encourage them to look to Director Krebs's example when considering his successor.

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 your experiences and your expertise.

Thank you Mr. Chairman.