SJC Crime and Terrorism Subcommittee Hearing
"How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors"
November 5, 2019
Opening Statement

Hackers, cybercriminals, and nation states are a persistent and growing threat – to individuals, private companies, critical infrastructure, and every level of government. While I am happy to hear from the witnesses here today about this important issue, I am disappointed that they will be the only people we hear from.

When Sen. Graham and I led this committee, we collaborated on a number of hearings to tackle the important issues facing the country, from the threat to our democracy posed by shell corporations to defeating fentanyl to cybersecurity. This is the first subcommittee hearing we've had this Congress, and I approached this hearing with the same spirit of collaboration and bipartisanship. As of last Friday, we were scheduled to hear from a very knowledgeable panel of government witnesses, including officials from DHS, DOJ, and the FBI. These officials have essential insight into how we should combat cyberthreats. Canceling their participation at the last possible moment is not a way to run a railroad. I hope we invite those officials back soon; I would still like to hear from them.

Today's hearing gives us the opportunity to review what we know about the cyber threats facing our country and consider what more we should be doing. When it comes to cyber security, we in Congress tend to fixate on what could happen when the government gets your data. We ought to think more about the private sector, its vulnerabilities, and how we can help address them. Here are a few places I think we could start:

We need to stress-test the NIST Framework to ensure it's actually improving cybersecurity outcomes. The NIST Framework, laying out voluntary best practices and industry standards for the private sector entities that operate and maintain critical infrastructure sectors, has been in use since 2014 – but we still don't really know if it's working.

We also need to ensure that law enforcement has the tools need to prosecute cybercrime.
Both cybercriminals and nation states continue to use botnets—zombie armies of compromised computers—for their cyberattacks. I've long championed legislation with Senators Graham and Blumenthal that would give law enforcement more powers to disrupt and prosecute these crimes.

Alongside aggressive, well-equipped law enforcement, we need to improve international standards for sharing information, and send a clearer signal to potential aggressors that the United States will impose consequences. An international "coalition of the willing" could agree to common international norms against cybercrime, state-supported hacking, and intellectual property theft, and hold accountable those states that transgress. We can't let bad actors frustrate our efforts to reach consensus with our allies about permissible state behavior in cyberspace.

Finally, we must do a better job of helping the public understand the scope and severity of cyber threats. The president should designate a cybersecurity "storyteller-in-chief," empowered to declassify information and charged with clearly, constantly, and concisely reporting known threats and attempted attacks. I have been happy to see DHS moving to share more information about recent cyberattacks, to do it faster, and to distribute that information to the public.

I look forward to discussing these issues with our witnesses, and I thank them for being here.