Committee on Energy and Commerce
Opening Statement as Prepared for Delivery
of
Subcommittee on Communications and Technology Ranking Member Doris Matsui

Hearing on "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era."

January 11, 2024

Thank you, Chairman Latta.

I'm excited that for our first hearing in 2024 we'll be exploring the modern cybersecurity landscape. It's timely and an important part of this Subcommittee's jurisdiction.

Over the last few years, major cyber events like the Colonial Pipeline and ransomware attacks on hospitals have opened Americans' eyes to the pervasive threat posed by unsecure cyber infrastructure. For too long, this threat was treated as an afterthought or something only major financial institutions needed to worry about. Unfortunately, recent history has shown just how flawed this mindset can be.

That's why I'm excited about hearings like this. It gives us an opportunity to remind the government, corporations, and consumers that cybersecurity must be a foundational consideration in the digital world. And even though the threats to critical infrastructure and corporations are receiving attention, I'm worried about the equally nefarious risks less-resourced organizations and consumers face.

I've been especially concerned about the rise in attacks targeting America's K-12 schools. The unfortunate reality is that cyberattacks targeting schools are increasing in frequency and severity. In 2016, the annual number of publicly disclosed cyber events was around 100. By 2021, that number had grown to nearly 1,400 annually. But, it's important to remember these are only the attacks that get publicly disclosed. Evidence suggests that 10 to 20 times more K-12 cyber incidents go undisclosed every year. 2021 was also the third straight year with more than 50 publicly disclosed K-12 ransomware attacks. Again, a number that in reality we know is much, much higher. These incidents have threatened students' privacy and caused harmful classroom disruptions. Alarmingly, many schools simply do not have the resources to adequately combat this sophisticated threat. That's why I introduced the bipartisan, bicameral Enhancing K-12 Cybersecurity Act.

My bill includes three provisions to promote access to information, better track cyberattacks nationally, and improve K-12 cybersecurity capabilities. First, it would establish a Cybersecurity Information Exchange to disseminate information, best practices, and grant opportunities to improve cybersecurity. Second, it would create a Cybersecurity Incident Registry to track incidents of cyberattacks on elementary and secondary schools across the country. Finally, and most importantly, it would deploy a K-12 Cybersecurity Technology Improvement Program to serve as a public - private partnership to boost K-12 cyber-defenses. I'm proud to say my bill has the support of major school groups like the National Association of

Secondary School Principals and Elementary School Principals as well as the Council of Chief State School Officers. Technology and industry groups are also on board like the Consortium for School Networking and the Information Technology Industry Council.

But, there is also plenty we can do administratively to give our schools a boost in their fight against cyber criminals. Back in 2022, I wrote to the FCC urging Chairwoman Rosenworcel to consider ways to modernize its E-Rate program to ensure it keeps pace with modern advances in cybersecurity. E-Rate currently allows for "basic firewalls" to defend against cyber attacks, this capability falls short of what is needed to address the cyber-threat landscape schools face today. Thankfully, this past July, Chairwoman Rosenworcel announced her plan to create a pilot program to invest in cybersecurity services for K-12 schools and libraries. This is an important step forward and I'm excited to work with the Chairwoman to ensure its success.

I'm also laser focused on what can be done to keep American consumers safe. In July, I joined Deputy national security adviser Neuberger and Chairwoman Rosenworcel at the White House to announce the Cyber Trust Mark. Like EnergyStar, this new mark will serve as a signal to consumers that the devices they're buying are safe. From baby monitors to smart thermostats, this will raise the bar in the internet of things.

I'm excited to hear from our witnesses today and with that I yield the balance of my time.