REMARKS OF
CHAIRWOMAN JESSICA ROSENWORCEL
FEDERAL COMMUNICATIONS COMMISSION
US CYBERSECURITY LABELING PROGRAM FOR SMART DEVICES
EISENHOWER EXECUTIVE OFFICE BUILDING
WASHINGTON, DC
JULY 18, 2023

Good morning. It's wonderful to be here with security champions in the government and so many industry experts, too.

There are now so many new devices—from smart televisions and thermostats to home security cameras, baby monitors, and fitness trackers—that are connected to the internet. These technologies provide huge benefits because they can make our lives easier and more efficient. They allow us to do things like check who is at the front door when we are away, keep tabs on our health, and automatically adjust the thermostat, so we save on our energy bills.

But this increased interconnection brings more than just convenience. It brings increased security risk. After all, every device connected to the internet is a point of entry for the kind of cyberattacks that can take our personal data and compromise our safety. That is true for the biggest connections to the largest businesses and the smallest connections to the devices in our homes.

Let me give you an example. This is from a story about cybercrime told by the author Misha Glenn. It involves a bank, which like most institutions in the modern economy, understood the vulnerabilities of digital age activity. In fact, they spared no expense when it came to cybersecurity. They carefully assessed the risks of their operation and spent liberally to ensure the secure transfer of funds. In the process, they convinced themselves that their comprehensive efforts had made them just about invincible. Of course, pride often comes just before the fall. Because despite their best efforts, it didn't take long for a hacker to find a vulnerability. It wasn't in the bank's systems for transactions, deposits, or accounts. It was in a vending machine at headquarters that was filled with chocolate bars. The vending machine had its own IP address. But the bank neglected to put it on the system for automated software patching updates. After all, when you plan for security updates, the machine where you drop your spare coins for something sweet to keep you going when working late is unlikely to be the focus of your efforts. But that was all it took for this bank to be penetrated. A single vending machine packed with chocolate.

I love this story because it is a reminder that so much is now connected in our lives. This is true in businesses—like banks—but it is increasingly true for all of us at home, too. All of those new home security cameras, connected thermostats, and fitness trackers add up. In fact, right now there are an estimated 17 billion smart devices in the world. And we are just getting started. Because the number of smart devices is growing fast. In fact, we expect to see 25 billion smart devices by the end of the decade. And cyberattacks on these devices are growing. They can make us wary of bringing smart devices into our lives, and missing out on the convenience and opportunity they provide.

But it doesn't have to be this way. Because we can do more to make internet of things devices secure and help consumers make good choices about what they bring into their homes and businesses.

In fact, a lot of people here today have been hard at work developing solutions. For years, my colleagues at NIST have been developing security criteria for smart devices. And last year, I had the opportunity to join many of you, along with NIST, for a discussion at the White House about how we can come together to improve security for smart devices and help consumers understand what they are purchasing.

I left that conversation energized. So now I want to tell you how we are going to turn that energy into action.

Today, I put before my colleagues at the Federal Communications Commission a proposal to put in place the first-ever voluntary cybersecurity labeling program for connected smart devices. We are calling it the U.S. Cyber Trust Mark. And just like the "Energy Star" logo helps consumers know what devices are energy efficient, the Cyber Trust Mark will help consumers make more informed purchasing decisions about device privacy and security. So when you need a baby monitor or new home appliance, you will be able to look for the Cyber Trust Mark and shop with greater confidence. What's more, because we know devices and services are not static, we are proposing that along with the mark we will have a QR code that provides up-to-date information on that device.

This proposal builds on good work already done by government and industry because we will rely on the NIST-recommended criteria for cybersecurity to set the Cyber Trust Mark program up. That means we will use criteria device manufacturers already know, and, when they choose to meet these standards, they will be able to showcase privacy and security in the marketplace by displaying this mark. Over time, we hope more companies will use it—and more consumers will demand it.

So let's talk next steps. If adopted by my colleagues at the agency, we will seek public comment on this proposal. We will ask for input on how best to establish this voluntary labeling program, the scope of eligible devices, the mechanics of managing this program, how to further develop standards that could apply to different kinds of devices, how to demonstrate compliance with those standards, and how best to educate consumers.

That is not a small task. But it's worth it. Because the future of smart devices is big. And even bigger is the opportunity for us to ensure that every consumer, business, and every bank with a vending machine can make smart choices about the connected devices they use. So let's get to it.