COMMISSIONER SIMINGTON ADDRESSES PLI
DECEMBER 6, 2023

Good morning. Thank you for the kind introduction and for inviting me to speak at this conference again.

A year ago, I discussed my view of widespread device security failures, my theory of FCC jurisdiction over the responsible parties, and some suggestions for possible courses of actions. A year later, we have now adopted an NPRM that takes a slightly different approach to the one I suggested, but which could still prove extremely effective at improving connected device security.

First, let's review where things stand with device security. Cybersecurity vulnerabilities are inevitable. Even the best engineers, supported by sophisticated organizations and applying the best software development methodologies, cannot hope to eradicate every security flaw lurking in a modern software-powered device, which these days could be a dishwasher, a traffic light, an airport WiFi router carrying the traffic of thousands, or a humble equipment cart, as much as a phone or computer. A single one of these vulnerabilities can be enough to render access controls and other security mechanisms useless, allowing even amateur attackers to bypass them and gain illicit access to sensitive information and controls. Because any device is liable to be rendered insecure at any time by a newly discovered flaw, a responsible manufacturer should undertake to diligently search for and patch vulnerabilities as quickly as possible. Otherwise, it might as well be putting ticking time-bombs into the homes and businesses of every one of its customers across the country.

Unfortunately, many device companies have fallen short. It often takes months for a fix to a serious vulnerability to make its way to end user devices, if the manufacturer bothers to release an update at all, and if the device was designed to be updateable in the first place. Manufacturers frequently pull the plug on support for a device well before consumers have stopped using it. The length of security support periods—the time period during which users can count on receiving timely security updates—is usually not communicated at the time of sale, and sometimes the end of support is not even announced, leaving even the most informed users unsure whether their devices are still safe to use. And many devices require manual installation of security updates, something very few consumers will ever do.

This is no mere academic concern. Attacks on unpatched devices are becoming more frequent and more dangerous. A recent FBI advisory warned of increasing cyberattacks against unpatched medical devices. Unpatched industrial control systems threaten the availability of critical infrastructure. The Mirai botnet, which at its peak consisted of over 600,000 compromised devices performing large-scale cyberattacks in unison, grew by scanning the internet for devices with unpatched vulnerabilities, like IP cameras and routers, and taking control of them. And we have not yet seen the worst. An attacker could use unpatched vulnerabilities to take control of large numbers of mobile phones, turn their radios into signal jammers, and take down mobile networks. Botnets of commandeered high wattage devices like air conditioners, water heaters, and ovens could be used to disrupt the power grid and even cause large-scale blackouts. And attacks on cyberphysical systems like automated cars, or on medical devices, can directly cause widespread property destruction, human injury, and death.

This situation is dismal. Peddling insecure or soon-to-be-insecure devices to consumers is irresponsible business conduct, and it’s high time to put an end to it. As I discussed last year, the FCC has the authority under Title III of the Communications Act to impose security requirements and liability on radio frequency-emitting devices, since security flaws in those devices can be used to cause harmful interference and affect the availability of wireless spectrum for public use. I still think the FCC can and should act in this way, but I won’t rehash those arguments today. Instead, I want to focus on the voluntary

US Cyber Trust Mark program announced by Chairwoman Rosenworcel in concert with other parts of the government which, despite being a less direct approach that still gives quarter to bad actors, has the potential be a strong first step that can lead to major improvements to the security of connected devices.

The premise of the US Cyber Trust Mark is simple. As a device manufacturer, you certify that your device meets a list of cybersecurity criteria, such as that you use modern secure communications protocols and implement secure authentication, and in exchange, you get to put a flashy US Cyber Trust Mark logo on your packaging and sales materials, effectively an endorsement from the federal government of the security of your product. In addition to the moral and persuasive authority of the federal government on such issues, the true value of the mark will probably come from organizations, including the federal government itself, adopting the mark as a requirement for their procurement of connected devices.

But for the mark to truly transform the security landscape, rather than just add another bureaucratic requirement to already convoluted and wasteful procurement policies, the program needs to be designed correctly.

First, the program cannot merely be a checklist of specific security features that a product must have. If security could be reduced to a list of criteria, then it wouldn't be such a continuing problem. Do you think that if there was some simple list of criteria for good security, that the most sophisticated organizations in the world would still continuously find themselves compromised by attacks on their internet-connected devices? They, and their insurers, would have adopted those criteria as requirements long ago, and major cyber intrusions would be a thing of the past. But that's not the world we live in. Which is not to say that lists of criteria cannot have utility. Many, such as FIPS, are respected by many organizations and do represent a good list of best practices, but they have nonetheless failed to stem the rising tide of cyberattacks.

The fundamental issue is that incentives matter, and as things stand now, device manufacturers and software vendors are rarely, if ever, held legally responsible for cybersecurity failures. In tort, products liability law only recognizes physical injury and death as bases for a cause of action. In contract and warranty law, sellers usually disclaim all liability for security failings at the point of sale. And more specific laws, like privacy laws, rarely make full damages from a breach recoverable, almost always lack private causes of action, and do not allow liable operators of online services to recover damages from negligent suppliers of software and devices, the way that a retailer found liable under product liability law can pursue recovery up the supply chain, up to and including from the original manufacturer.

Yet another checklist compliance exercise won't change any of this, and if that's all that comes out of this program, it would be a tremendous waste of time and money. Instead, the strongest promise of the Cyber Trust Mark program is that it will create a legally enforceable contract between the seller and buyer of the connected device. The content of this contract should not just include representations about the product at a snapshot in time—that it uses a particular kind of encrypted communications protocol, that it is capable of being updated, that it supports user authentication, that it has no known vulnerabilities—but also promises about further action that the manufacturer will take, such as that it will provide security patches until at least a particular date, that it will continue to diligently search for vulnerabilities, and that it will maintain the security of any online services that support the product.

Second, the goal should not be to hand out as many cyber trust mark certifications as possible. The purpose of USDA's beef grading program is not to hand out as many Prime labels as possible. Likewise, the purpose of NHTSA's car safety program is not to give as many five-star ratings as possible. To paraphrase a former President, obtaining these labels has meaning not because it is easy, but because it is hard. Unfortunately, some are trying to steer the cyber trust mark program in an unambitious direction, into a list of vague criteria that only the most flagrantly irresponsible manufacturers would not already be in compliance with. Under these proposals, only the cybersecurity equivalent of a Trabant or Yugo would fail to receive the US Cyber Trust Mark.

The fact of the matter is that the device security landscape is so dismal that the government should be happy to deny the trust mark to most devices on today's market. Only the most responsibly designed and supported products should be eligible for the US Cyber Trust Mark. The mark should represent not just the state of the art of best security practices at the time the device as sold, within the limitations of what a checklist of requirements can hope to measure, but evidence that the manufacturer has put their skin in the game. An end consumer or business buying a cyber trust mark product should have the confidence that if the product fails to live up to that promise, they are entitled to a refund, or if they have suffered further harm, recovery for it.

So it is okay if, at first, devices with the cyber trust mark are relatively rare and expensive. The cyber trust mark should become a requirement for federal government procurement, which will immediately create a market for these products. Major corporations and other organizations with elevated security requirements will likely follow suit. And in that way, the market for these products will grow over time. Economies of scale will make these products increasingly desirable and available in the consumer market, as consumers become willing to pay a little more for a product with the coveted trust mark than for one without it. This is what raising standards through a voluntary program looks like, and we shouldn't trade this path to success away for the sake of a quick paper victory where every device on the shelf has the mark in two years and manufacturers heap praise on the FCC for helping them profiteer by peddling fake security to consumers. I suspect that some manufacturers will choose to not pursue a label rather than commit themselves to doing the right thing. Personally, I will avoid such products.

Third, receiving the US Cyber Trust Mark should not give a manufacturer a shield from liability. Many device manufacturers would like to be able to use the mark as a defense in state and federal court when security flaws in their devices lead to damaging attacks anyway. Like I already explained, no list of criteria can ever substitute for the constant vigilance and thoughtfulness of good engineers and business leaders. Good security is a constant process, and it requires skin in the game. It is only through ex post responsibility for failures that the legal system can create the incentives for good behavior. So, proposals for a safe harbor have it totally backwards. The greatest value of the trust mark is not the list of criteria that must be met to get it, but the ongoing legal commitment it creates for recipients to take the security of their products seriously. A safe harbor, or any kind of preemption of other liability regimes, would undermine that.

Unsurprisingly, not everyone is thrilled with my proposal. One critique that I've been confronted with is that my proposal would have FCC stifle an innovative industry with the weight of bureaucracy and compliance exercises. This is a valid concern about regulation generally and is in fact part of the reason why I think the focus of the program should be more on ex post liability rather than ex ante prescriptive checklists. Neither the FCC nor any other standard setting organization can possibly hope to keep up with rapid innovations in device security. An engineer who develops a more secure protocol, a better encryption algorithm, or a more secure programming language should not have to wait for regulatory approval to use it in a product. If it is indeed a thoughtful design, he can rest assured that he will have an opportunity to justify his actions should they ever be challenged in a lawsuit. This is how the products liability tort regime works, and it has successfully raised the bar for product safety in the American market, the most vibrant and innovative product market in the world. I want to extend that same success to device security.

Like I said last year, I’m a Republican and a free marketeer. But the free market requires that negligent sellers who cause harm by putting dangerous products into the world be held legally responsible. It is simply not possible for the purchasers of connected devices to adequately evaluate the security of devices before they buy them. Most devices are closed source, and even if they were open source, it would be implausible to perform a source code audit of every single bit of software in every device. And even a full source code audit could not guarantee the security of a device. Security is inherently a never-ending process, not an end-state. There will always be newly discovered vulnerabilities and the need for the manufacturer to issue security updates. Someone has to take responsibility for this process, and it can’t be every single person who buys a wireless device. The only plausible party is the device manufacturer.

So, I encourage the industry to support my proposals. To the responsible device manufacturers of the world, this is an opportunity to differentiate your product from the trash products that undercut your investment in good security and make it hard for you to profit from good engineering. To American businesses and institutions, this is an opportunity to foster an ecosystem of products whose manufacturers have skin in the game for your security, whose manufacturers will be partners in keeping you and your customers safe from cyberattacks. To end consumers, this means your privacy and finances will be more secure. And to the country, this means less susceptibility to debilitating botnets and foreign attackers seeking to cause mayhem and debilitate our economy.

Thank you for listening to me today. I look forward to answering any questions you might have. I’d love to discuss this particular issue more, but I’m also happy to take questions about other FCC matters as well.