Tobin Richardson, President and CEO, Connectivity Standards Alliance

Before the

House Committee on Energy and Commerce
Subcommittee on Communications and Technology

January 11, 2024

Chairman Latta, Ranking Member Matsui and members of the Subcommittee, my name is Tobin Richardson, I am President and Chief Executive Officer of the Connectivity Standards Alliance – the international standards body for the Internet of Things industry. I have nearly 30 years of professional experience and expertise in the technology industry and have led the Alliance since 2014.

The Alliance is comprised of more than 700 member companies that connect consumers to the world of devices. Our goal is to improve this connection between people and devices to promote innovation in the most secure environment possible.

This connection between people and devices is already delivering big benefits for the American people. Just to name a few, smart water pressure sensors alert consumers to water leaks so they can be fixed before destroying a lifetime of memories. Smart locks give families peace of mind that their home is secure and that the kids are behind locked doors. Smart thermostats help control energy costs, promote sustainability, and entry sensors help stop home invaders. Historically, the Internet of Things has been characterized by custom solutions and custom hardware. If you wanted smart light bulbs, you needed the smart light bulbs, their associated gateway device, and an app to control them all. This was not only a challenge for consumers trying to make things work together in their homes, but it also created the challenge

of evaluating the relative security risk of each piece of technology in their homes and whether their personal data would be kept private and secure.

Some of our member companies engaged early to help consumers navigate the dizzying complexity of integrating different systems interfacing in unique ways by creating ecosystems of devices that could work together within the home. Amazon's 'Works with Alexa', Apple's HomeKit, Google Home, and Samsung SmartThings are the largest and best known, but there were and are other ecosystems of devices competing for IoT consumers. This was a significant improvement over hundreds of separate options, but as an industry we thought we could do better. That improvement is called Matter.

While still in its infancy, today our Matter Standard is allowing consumers to connect smart devices from different manufacturers across the industry. Matter does this by using a common application layer and data model that delivers interoperability between devices allowing them to communicate with each other across multiple network technologies. At launch, Matter supported Wi-Fi, Thread, and Ethernet for connecting devices to consumers home networks. While this has certainly made it easier for consumers to work across the various voice assistants, app stores, and applications it has also allowed us to work together to promote integrated security and privacy.

As Matter was developed by our membership, integrating data privacy and security was essential to our work. That's why the Alliance developed a set of principles to guide this global standardization work. Those principles are:

- Confidentiality and Integrity - Using strong cryptographic standards to help protect data communicated between Matter devices

- Proof of identity - Using cryptographic certificates to ensure that data is shared only between known Matter entities
- Open Standard - Enabling anyone to inspect the template for Matter interactions between legitimate Matter nodes
- Minimizing data shared – Sharing data for specific operations of devices as required by Matter reducing the potential for inadvertent data leakage to protect consumers' privacy

These principles aim to protect consumers and their personal information in IoT systems. We applaud this Committee for its work on IoT cybersecurity and believe our principles are consistent with those efforts.

As our members developed Matter, we recognized that if we truly believe in providing an environment for data privacy, we must ensure that security is at the heart of the Matter standard. This is why security was core to the development of Matter; security is essential to the operation of Matter devices; and importantly Matter creates a baseline for device security that consumers can understand.

Just as we started with principles for our privacy work, the Alliance's principles on security serve as key design tenets and provide a baseline for building secure IoT devices. I would like to briefly describe these five principles.

- First, Matter devices employ a ***comprehensive*** security approach. That means securing the device from the start, protecting every message the device sends from the moment the consumer adds it to their network, and ensuring that updates to the device are secure.

- Second, security of Matter devices is based on ***strong***, established cryptography out of the box.
- Third, Matter devices need to be ***agile***. As others on this panel have testified, cyber threats are constantly changing. Device security needs to be at least as adaptive as the threats it will face.
- Fourth, Matter devices need to be ***resilient***. Even the most well-designed device will face adverse conditions. These devices need to be designed to protect themselves, detect threats, and recover from failures.
- Finally, all of this has to be ***easy***. Consumers should not have to be part-time engineers. Matter devices must handle this security challenge in a way that is consumer-friendly, easy to implement, and easy to use. For instance, with Matter, consumers now don't need to download security updates, those updates are pushed automatically to devices.

In addition to building consumer confidence with Matter, we support the Federal Communications Commission's (FCC) proposed U.S. Cyber Trust Mark program. We believe this program will be most effective if it remains voluntary and focused on IoT devices. We also recommend the FCC structure the program to allow it to:

- Be strong enough to meaningfully address IoT security;
- Be flexible enough to incentivize private sector adoption; and
- Be informative enough for consumers when they purchase new products.

The Alliance looks forward to working with the FCC and our colleagues in the industry, such as the Consumer Technology Association, on implementing this program. In fact, we have been working for the last two years to develop a certification program based on the existing NIST

standards for IoT security and on similar standards that have been developed in Europe and Singapore. Our program will enable manufacturers to certify their products once and verify that they comply with the requirements of the USA, Singapore, and Europe.

With this unified approach, consumers will have a new tool that will give them confidence that the products they are purchasing meet baseline cybersecurity requirements. They can just look for the new FCC label. And manufacturers will have a cost-effective way to check once that they comply with IoT security rules in the US and other countries.

Our members are proud to support strong IoT security in their products and in standards. With the new US Cyber Trust Mark, consumers will be informed about product security and thus empowered to choose solid security for their smart home.

Thank you again for this opportunity to testify today and I look forward to your questions.