December 16, 2021

NIST RFI Response for CSA

Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward

The **Connectivity Standards Alliance** (CSA), formerly known as the Zigbee Alliance, is submitting these comments for both of the following RFIs as they relate to each other and have interdependencies as they relate to Internet of Things (IoT) ecosystems. Accordingly, these comments are responsive to both subject matters.

- **DRAFT Baseline Security Criteria for Consumer IoT Devices**, August 31, 2021, published at: https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf; and
- **Consumer Cybersecurity Labeling for IoT Products: Discussion on the Path Forward**, issued December 2, 2021, published at: https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf

Established in 2002, the CSA is the foundation and future of the IoT. CSA's wide-ranging global membership collaborates to create and evolve universal open standards for the products transforming the way we live, work and play. With the Alliance's Members' deep and diverse expertise, extensive and robust certification programs, and a full suite of open IoT solutions, CSA is leading the movement toward a more intuitive, imaginative, and useful world. The Connectivity Standards Alliance board of directors is comprised of executives from **Amazon, Apple, ASSA ABLOY, Comcast, Google, Huawei, IKEA, Infineon, The Kroger Co., LEEDARSON, Legrand, Lutron Electronics, NXP, OPPO, Semiconductors, Resideo, Schneider Electric, Signify** (formerly Philips Lighting), **Silicon Labs, SmartThings (Samsung), Somfy, STMicroelectronics, Texas Instruments, Tuya**, and **Wulian**. Find out more about the Alliance at **www.csa-iot.org**, and about Matter at **www.buildwithmatter.com**.

CSA supports the goals of Executive Order 14026, Improving the Nation's Cybersecurity, and appreciates NIST's ongoing efforts to improve IoT cybersecurity. Cybersecurity is a substantial concern for IoT consumers and a top priority for the CSA. In response to the NIST request for feedback on a consumer IoT labeling program, CSA agrees with the use of NISTIR 8259 as the

foundation for the program. Further, the CSA agrees with the approach to not define a US Government label but rather to define desired outcomes that can be used as inputs by external labels and label certification programs. Consumers and manufacturers will benefit from having a small number of IoT cybersecurity labeling programs that are recognized in multiple jurisdictions across the globe.

The CSA believes that the product centric approach articulated by NIST, namely, requiring outcomes to be embodied in device, gateway, cloud, and apps, would have significant benefits, but driving to ensuring cybersecurity across these various elements of how consumers are delivered products may be challenging. For instance, while some manufacturers may control some or many of these delivery elements (device, gateway, cloud or app), only some of these manufacturers of IoT products may be able to ensure that the cybersecurity outcomes defined by NIST are achieved across all these components, and a labeling scheme may be able to communicate this to consumers. However, the market reality is that with widely adopted IoT standards, most homes will include a mix of devices, gateways, clouds, and apps from different manufacturers. The challenge of verifying cybersecurity outcomes in such a mixed, hybrid and diverse environment will increase or may not be achievable at all. However, the IoT standards that enable secure interoperability (such as those that the CSA has developed and is developing with leading tech companies) can provide the key to unlocking this dilemma by enabling secure system properties across products from multiple vendors.

In summary, CSA is approaching the challenges of IoT cybersecurity with enthusiasm. Our technologies and capabilities can provide critical building blocks that can be used to create more secure IoT systems.

With respect to layered labeling, CSA agrees with the approach to start with a binary label + QR Code labeling approach for consumer-based IoT products. The CSA believes it is important to distinguish labels from marks such as UL or CE marks since IoT devices will likely have different levels of security requirements and market needs. A label best serves the consumer when it means the device is designed to achieve the appropriate level of security for that type of device. NIST has established a clear baseline for components that provides a starting point for cybersecurity rating. CSA believes that this labeling approach will encourage adoption and ongoing use of the baseline requirements which are necessary to provide improved cybersecurity for consumers.

CSA is well-positioned to be able to tailor product criteria for different IoT device types, define conformity assessment, develop a label and associated information, and conduct outreach for products in consumer IoT. CSA certification programs today are well-developed and understood in the marketplace, and cover protocol conformance. Security specifications and test materials and programs to ensure conformance to specifications through evaluation and attestation programs is already under development within the Alliance.

CSA appreciates the opportunity to provide comment to NIST on these important topics, and has programs in place (as well as in development) to work with and augment NIST initiatives. CSA stands ready to further collaborate with NIST as the leading IoT standards development organization.

Kind regards,

Tobin Richardson
Chief Executive Officer
Connectivity Standards Alliance