September 30, 2019

Michael Fagan
Katerina Megas
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via email to: iotsecurity@nist.gov

Re: Comments on Draft NISTIR 8259, Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

Dear Mr. Fagan and Ms. Megas:

BSA | The Software Alliance[1] appreciates the opportunity to provide comments on the National Institute of Standards and Technology's (NIST's) Draft NIST Interagency Report 8259, "Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers" (Draft). BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members are at the forefront of software-enabled innovation that is fueling global economic growth and advancing the development and deployment of the Internet of Things (IoT). As global leaders in the development of data-driven products and services, and in promoting and strengthening cybersecurity, BSA members are committed to securing IoT devices in today's connected world.

BSA also appreciated the opportunity to comment on an earlier version of the Draft, "Considerations for a Core IoT Cybersecurity Capabilities Baseline." While BSA recognizes the importance of focusing on security capabilities or features for IoT devices, as NIST did in the earlier version, effective IoT security demands a holistic, lifecycle approach. BSA applauds NIST's inclusion of additional considerations, such as guidance on secure development lifecycles and communication of critical security information to customers, in the current Draft. Preventing weaknesses and vulnerabilities in IoT devices can only be

[1] BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

effectively addressed through discussion of both product capabilities and the underlying technical features, including software, hardware, and firmware.

In particular, BSA commends NIST's inclusion of IoT device lifecycle considerations and secure development practices in the Draft. The Support and Lifespan Expectations and Decommissioning discussions in Section 6 of the Draft help IoT device vendors plan and maintain guidance for a product's end-of-life. End-of-life considerations are a significant element of IoT device security since out-of-date IoT products are more likely to be vulnerable to hackers and bugs. Furthermore, the continued use of unsupported IoT devices or the abrupt termination of support to devices could be problematic.

Additionally, the notation of NIST's recent software security white paper, "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)," and its references in Section 7 of the Draft encourage IoT device security to be approached in a holistic manner that acknowledges the importance of both the capabilities of a product and its underlying elements. The Draft's additional guidance, combined with Section Four's Core Baseline for IoT Devices, represents a good first step in developing foundational recommendations for IoT security.

BSA looks forward to working with NIST to build on these discussions in future iterations. Furthermore, as NIST continues to refine the Draft, BSA suggests two modifications to clarify the Draft's guidance and refine its scope. First, NIST should create and include in the Draft a definition of "IoT device." Given NIST's expertise in the IoT and security, NIST's definition of "IoT device" would be particularly helpful to policymakers as they draft and consider proposals relating to IoT devices and IoT security. Additionally, because the Draft is centrally focused on security for *IoT devices*, NIST should define what exactly is addressed by the document's guidance. Many of the Draft's stated definitions, which are important in clarifying and targeting the guidance NIST provides (namely: "actuator," "authorized entity," "cybersecurity event," "entity," "interface," "IoT platform," "local interface," "local logical access," "minimally securable IoT device," "network interface," "remove logical access," "sensor," and "transducer"), use the term "IoT device" as part of the definitions, leaving those definitions vague as well. Defining "IoT device" will provide clarity to these definitions and the overall Draft, making NIST's guidance more meaningful and actionable. Also, the definition of "IoT device" should clearly distinguish between components and finished products in the context of the Draft. A device, under these circumstances, is a finished product available to consumers that is usable for its intended functions without being imbedded or integrated into any other product and is not a component.

Second, NIST should revise the Data Protection Feature in Section 4 of the Draft to clarify that data should be protected in accordance with a data protection strategy that determines the sensitivity of the data and how it should be protected. The need for and type of protection

may be determined based on the data being collected, the context of collection, and other risk factors. Because some IoT devices gather data of little importance or with little temporal value, not all data needs to be protected.

BSA and its members look forward to working with NIST to encourage more robust security measures across the IoT industry. Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org