February 7, 2020

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

Via email to: iotsecurity@nist.gov

Re: Comments on Draft (2nd) NISTIR 8259, Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline

Dear Mr. Fagan, Ms. Megas, Ms. Scarfone, and Mr. Smith:

BSA | The Software Alliance[1] appreciates the opportunity to provide comments on the National Institute of Standards and Technology's (NIST's) Draft (2nd) NIST Interagency Report 8259, "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline" (Second 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 earlier versions of the report and recognizes the importance of focusing on security capabilities or features for IoT devices. BSA members believe effective IoT security demands a holistic, lifecycle approach that builds consideration and mitigation of risk into processes spanning from a project's inception through the end of its life. Moreover, though we understand that the draft NISTIR 8259 is focused on providing device customers with capabilities to secure the devices, we believe

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

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

preventing weaknesses and vulnerabilities in IoT devices can only be effectively addressed through discussion of building security into both product capabilities and a product's underlying components, including software, hardware, and firmware.

BSA appreciates the intent of the drafters in the Second Draft to articulate a series of activities designed to help device manufacturers improve how securable an IoT device is for customers. However, the Second Draft's organization is less clear and less concise than the earlier version of the report. The Second Draft's use of "Foundational Activities" implies a broad review of considerations central to IoT device security, much broader than what is examined in the Second Draft. BSA suggests reverting back to the structure of the first draft report, a clearly identified core baseline of cybersecurity features for IoT devices followed by additional security considerations for IoT device manufacturers; or broadening the scope of the Second Draft to include a much more comprehensive consideration of foundational security activities for IoT devices, such as supply chain risk management for all aspects of the IoT device (software, hardware, and firmware).

Moreover, BSA appreciated the previous draft's discussion of secure development lifecycle (SDLC) concepts and their importance to the software, hardware, and firmware components of a device. While many individual concepts or elements of an SDLC are discussed in the Second Draft, the document's less focused approach sacrifices both clarity and emphasis on these important concepts. The Second Draft accurately states that, "Improving how securable an IoT device is for customers means helping customers meet their risk mitigation goals, which involves addressing a set of risk mitigation areas." Yet, improving how securable an IoT device is will also mean considering and mitigating risk in the design and production of the device, regardless of whether these mitigations are intended to interact with customers. From this standpoint, the decreased focus on an SDLC is concerning. Also concerning is that the document suggests that secure development practices such as minimizing vulnerabilities and securing third-party software components are optional, noting that "Manufacturers should consider which, **if any**, secure development practices are most appropriate for them and their customers." If this guidance is to succeed in guiding the development of more secure and securable IoT devices, such secure development practices will be essential and should be strongly encouraged.

Finally, BSA commends NIST's explanation of the IoT devices in scope for the Second Draft. Because the Second Draft is focused on security for *IoT devices*, NIST's statement regarding the devices in scope provides clarity to the document's guidance. To further clarify NIST's explanation, BSA suggests revising lines 286 to 289 of the report to read as follows: "The IoT devices in scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world, and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world. The IoT devices in scope for this publication can function on their own.

Components of another device, such as a processor, are not able to function on their own in this context and are not an IoT device." Moreover, to provide additional clarity BSA recommends including this explanation as a definition for "IoT Device" in the Second Draft's glossary, Appendix B, with the proposed edits above.

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