February 23, 2021

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via email to: iotsecurity@nist.gov

Re: Comments on Draft NISTIR 8259B, 8259C, 8259D, and Draft NIST SP 800-213

Dear Mr. Fagan, Mr. Marron, Mr. Brady, Ms. Cuthill, Ms. Megas, and Ms. Herold:

BSA │ The Software Alliance[1] appreciates the opportunity to comment on the National Institute of Standards and Technology (NIST)'s Draft NIST Interagency Report (NISTIR) 8259B, "IoT Non-Technical Supporting Capability Core Baseline," Draft NISTIR 8259C, "Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline," Draft NISTIR 8259D, "Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government," and Draft NIST Special Publication 800-213, "IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements" (collectively, the "Draft Guidance").

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members provide products and services that other companies rely on, including cloud storage solutions, human resources management, identity management services, and customer relationship management. As leaders in the global technology industry, BSA members are at the forefront of IoT innovation, including advancements in IoT security.

Inadequately secured IoT technologies can serve as entry points for cyberattacks, compromising sensitive data and threatening the safety of individual users. Attacks on

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

infrastructure and other systems, fueled by networks of poorly secured IoT devices, can affect the delivery of essential services, put the security and privacy of others at risk, and threaten the resilience of the Internet globally. BSA recognizes the importance of securing IoT technologies and commends NIST's valuable work to strengthen the security of IoT devices.[2] NIST's ongoing IoT security efforts represent an important step forward in mitigating the risks posed by inadequately secured IoT devices. As NIST further refines the Draft Guidance, BSA offers the following recommendations.

Recommendations from NIST's SSDF White Paper

Preventing weaknesses and vulnerabilities in IoT devices can only be effectively addressed through discussion of both product capabilities and the underlying technical features, including software, hardware, and firmware. BSA commends the Draft Guidance's consideration of software security, including through its discussion of secure software development practices, secure supply chain practices, and software updates. BSA members pioneered many of today's software security best practices and have been industry leaders in developing the concept of the secure development life cycle (SDLC). An SDLC—including vendor commitments to embrace secure development best practices, manage supply chain risk, mitigate identified vulnerabilities, and address end-of-life considerations—is critical for the software, hardware, and firmware elements of IoT devices. NIST has also done valuable work developing recommendations on secure software development practices in its White Paper on "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)" (SSDF White Paper). The SSDF White Paper provides important foundational guidance for a core set of high-level secure software development practices to be incorporated with each SDLC implementation. Given the importance of software security to IoT device security, BSA suggests NIST more thoroughly integrate the recommendations from its SSDF White Paper into the Draft Guidance. Many of the practices outlined in the SSDF White Paper are relevant to the software used in IoT devices and can provide valuable guidance in creating more secure IoT software, which creates more secure IoT devices.

Internationally Recognized Standards

Several internationally recognized technical security standards are applicable to IoT technologies and provide widely vetted, consensus-based information and guidance for defining and implementing effective security methodologies. Consensus-based, internationally recognized security standards also facilitate common approaches to common challenges, thus enabling collaboration and interoperability. Security standards promote interoperability across various use case deployments, vendors, sectors, and geographies, which will maintain the long-term viability of the IoT and encourage the equitable distribution of the benefits and security of IoT solutions. Employing greater interoperability and the use of open, voluntary, and widely available standards as technical building blocks for IoT devices

[2] For more information on BSA's IoT security efforts, see the BSA Policy Principles for Building a Secure and Trustworthy Internet of Things, https://www.bsa.org/policy-filings/bsa-policy-principles-for-building-a-secure-and-trustworthy-internet-of-things.

will support greater user benefits, innovation, and economic opportunity. BSA encourages the exercise NIST is undertaking in incorporating informative references into the Draft Guidance and suggests NIST map its recommendations to consensus-based, internationally recognized security standards wherever they exist. Similarly, NIST should strongly encourage those creating a profile based on the Draft Guidance to review consensus-based, internationally recognized security standards to enable better security outcomes.

Strongly Encouraging Non-Technical Supporting Capabilities

NISTIR 8259B provides additional, non-technical support guidance to IoT device manufacturers in the IoT Non-Technical Supporting Capability Core Baseline. The baseline addresses several critical aspects of IoT device security, including the manufacturer's: documentation of relevant security information through the IoT device's development and lifecycle, ability to receive security-related information and queries, communication of security information, and security education and awareness efforts. While BSA agrees the non-technical supporting capabilities outlined in the baseline should not be mandatory, to provide IoT device manufacturers with sufficient flexibility in crafting their security approaches, BSA recommends NIST strongly encourage these activities, rather than suggesting "[t]he individual non-technical supporting capabilities in the baseline may be implemented in full, in part, or not at all." Many of the baseline's non-technical supporting capabilities, including those related to secure software development and supply chain practices, software updates, processes for receiving maintenance and vulnerability information, and device lifespan and term of support, are essential to IoT security and will improve the security of IoT devices if incorporated by manufacturers.

BSA looks forward to continuing to work with NIST to promote security throughout the IoT ecosystem. Thank you for the opportunity to comment on this important matter.

Sincerely,

Meghan Pensyl

Meghan Pensyl
Manager, Policy
BSA │ The Software Alliance