



May 28, 2019

Katerina Megas  
Program Manager  
Cybersecurity for Internet of Things Program  
National Institute of Standards and Technology  
100 Bureau Drive  
Gaithersburg, MD 20899

Via email to: [iotsecurity@nist.gov](mailto:iotsecurity@nist.gov)

**Re: Comments on Considerations for a Core IoT Cybersecurity Capabilities  
Baseline Discussion Draft**

Dear Ms. Megas:

BSA | The Software Alliance<sup>1</sup> appreciates the opportunity to provide comments on the National Institute of Standards and Technology's (NIST's) Considerations for a Core Internet of Things (IoT) Cybersecurity Capabilities Baseline discussion draft (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 IoT. As global leaders in the development of data-driven products and services, and in advancing cybersecurity, BSA members understand the importance of securing IoT devices in today's connected world.

BSA supports NIST's efforts to develop foundational recommendations for IoT security. This effort could lead to a useful operational guide that promotes risk-based approaches to security and clarifies IoT best practices. With both manufacturers and products in the IoT market expanding rapidly, such guidance is urgently needed.

BSA provides the recommendations below to refine the Draft's scope and improve its clarity. First, however, we should emphasize one important consideration around which several of our recommendations revolve: the need to incorporate indicators relating to security in IoT product development in addition to pre-market capabilities. The Draft differentiates between "pre-market cybersecurity capabilities that could be built into products" and "cybersecurity controls that consumers could apply post-market." This approach, however, risks neglecting

---

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

a critical element of IoT device security: preventing weaknesses and vulnerabilities. Capabilities, as the document notes, are functions or features of a product that enable it to achieve a specific security goal – features such as encryption modules, identity and access management mechanisms, or capabilities to implement updates securely. Such capabilities are certainly important to securing IoT devices; however, even the adoption of the most robust security features cannot protect devices against vulnerabilities in poorly developed software or hardware. Therefore, BSA believes that an IoT security baseline, to be effective, must address both the capabilities of a product and the underlying components, including software, hardware, and firmware.

In light of this principle, BSA recommends the Draft incorporate guidance regarding secure product development to improve its completeness and utility. Below, we emphasize the importance of incorporating security-by-design principles through a focus on a secure software development lifecycle; specifically, we recommend highlighting the importance of established processes for supply chain risk management, vulnerability management, and end-of-life guidance. Though BSA's comments focus on applying secure product development lifecycle principles to software, such principles are applicable to hardware and firmware components of IoT devices as well. In addition, BSA recommends NIST seek to align its efforts with other current IoT security initiatives around the world to encourage global policy harmonization and advance NIST's position as an international leader on IoT security.

### **Secure Software Development Processes**

As the May 2018 Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats noted, "Devices must be able to resist attacks throughout their deployment lifecycles—at the time of shipment, during use, and through to end-of-life. For this to occur, security must become a primary design requirement." Achieving this goal means, as the report recognized, encouraging the widespread adoption of industry best practices, particularly in the form of security-by-design principles integrated into secure development lifecycle methodologies.

NIST should incorporate security-by-design principles into its Draft to ensure security considerations are integrated into the software powering IoT devices from the software's inception throughout its lifecycle. As a representative of companies that pioneered leading software security best practices, BSA strongly supports the adoption of security-by-design principles as a basis for ensuring software products are securely developed and securely maintained. Security-by-design principles guide developers to build security considerations into the entire software development process, which leads to better quality software with fewer vulnerabilities. They include principles such as "least privilege," ensuring that only the access privileges granted are the minimum required for a task; "secure failure," ensuring that software modules can fail without exposing data or creating unauthorized access; and "secure default," ensuring that initial configurations of software provided to users are as secure as possible.

These security-by-design principles should be incorporated into software development life cycle (SDLC) concepts in the Draft. A SDLC is generally a series of steps, or phases, that provide a framework for integrating security into software development and managing it through the software's entire lifecycle. Although a SDLC does not prescribe a specific technique or single way to develop applications and software components, there are



established methodologies that organizations use and models organizations follow to address different challenges and goals. A SDLC provides some level of control of the development process to ensure the design and testing processes leading to release of a product are well-managed and documented, maximizing organizations' ability to produce secure software in a verifiable, repeatable, transparent manner.

Recently, BSA published the *Framework for Secure Software*, a first-of-its-kind tool for describing and assessing software security through a flexible, outcome-based, risk-informed methodology. The BSA Framework addresses both organizational processes and product security capabilities to inform and assess software security throughout its lifecycle. The Framework focuses on three functions, which organize fundamental software security activities at their highest level: Secure Development, Secure Capabilities, and Secure Lifecycle. Many topics discussed within the Secure Capabilities function are also addressed in Capabilities 1-8 of the Draft, including patchability, authorization and access controls, encryption, and logging. Security-by-design principles and SDLC concepts are described holistically within the BSA Framework; the Framework may be a useful reference as NIST continues to develop its IoT security baseline. Moreover, it will be important for NIST to ensure that the Draft discussed here is informed by, integrates, and informs NIST's ongoing work to develop secure software development lifecycle guidance, as directed in the November 2018 *Road Map Toward Resilience Against Botnets*.

In addition to generally addressing secure software development, BSA would like to highlight three key elements of an effective SDLC that are particularly important to IoT security and apply to hardware and firmware in addition to software: supply chain risk management, vulnerability management, and end-of-life policy.

➤ ***Supply Chain Risk Management***

As one key element of an SDLC, NIST should address supply chain risk management in the Draft. The IoT supply chain includes the processes and components incorporated into producing, tracking, and maintaining the device and its components. Since software is a key component of IoT devices, software supply chains must be secure to ensure the security of an IoT device's supply chain. Robust software supply chain security practices include software development processes that are informed by supply chain risk management and measures to ensure the security of third-party components integrated into the software. NIST should incorporate these supply chain considerations in the Draft.

➤ ***Vulnerability Management***

Vulnerability management is another important element of the SDLC that should be emphasized in an IoT cybersecurity baseline. Recognizing that the Draft seeks to differentiate between pre-market considerations and controls to be adopted by consumers, it is important to note that establishing effective, systematic processes for identifying, mitigating, and learning from vulnerabilities should occur during the development stages of a product. Moreover, vulnerability management is not a control that a consumer can apply, but a critical responsibility of the product developer/vendor. Vulnerability management generally refers to the continuous process of discovering, assessing, prioritizing, and mitigating software weaknesses. Organizations should have a vulnerability management plan outlining policies, responsibilities, and expectations for both internal and external stakeholders



throughout the IoT product's lifecycle. Vulnerability management is a vital, basic tenant of a robust and comprehensive security approach and should be reflected in the Draft.

➤ **End-of-Life**

Finally, SDLC guidance in the Draft should address end-of-life considerations. End-of-life is a term used to describe when a product supplied to customers is at the end of its useful life (from the vendor's point of view) and the vendor stops marketing, selling, or sustaining the product. Vendors of IoT devices should plan and maintain guidance for a product's end-of-life, which may include communicating to customers reasonable expectations for the nature and lifespan of product support, because continued use of unsupported IoT devices or the abrupt termination of support to certain devices could lead to several problems. For example, some IoT devices serve safety roles, and malfunctions could lead to injury, property damage, and theft, especially if consumers are unaware of product limitations. Moreover, out-of-date IoT products are more likely to be vulnerable to hackers and bugs, which could create vulnerabilities for other systems connected to these IoT devices. Consequently, end-of-life is an important component of IoT security and should be included in the Draft.

**Alignment with Other Efforts**

As NIST's work on the Draft continues, BSA encourages NIST to ensure that its work is informed by and, to the extent possible, aligned with other, similar efforts currently underway around the world. For example, the European Union Agency for Network and Information Security has developed a robust workstream on IoT security, including the publication of Baseline Security Recommendations for IoT and a current initiative to develop an IoT security certification scheme under the recently passed *Cybersecurity Act*.<sup>2</sup> Additionally, the United Kingdom's Department for Digital, Culture, Media and Sport and the National Cyber Security Centre recently worked with industry partners to develop a voluntary Code of Practice for Consumer IoT Security to improve cybersecurity and consumer safety.<sup>3</sup> Other governments, such as Singapore and Japan, have announced plans to develop IoT security guidelines.

As these efforts take shape, multinational technology companies developing IoT devices and their components will face an increasingly complex landscape of policy guidance, regulatory requirements, and standards. Such businesses will be harmed by an international policy landscape that is disjointed, incoherent, and conflicting; such an outcome will suppress innovation and competitiveness. Harmonizing global approaches to IoT security is a critical goal, and NIST is well-positioned to lead in this respect.

---

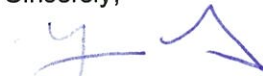
<sup>2</sup> European Union Agency for Network and Information Security (ENISA), Baseline Security Recommendations for IoT (Nov. 2017), available at <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>; See also ENISA, IoT Security Standards Gap Analysis (Jan. 2019), available at <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

<sup>3</sup> United Kingdom Department for Digital, Culture, Media and Sport, Code of Practice for Consumer IoT Security (Oct. 2018), available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/773867/Code\\_of\\_Practice\\_for\\_Consumer\\_IoT\\_Security\\_October\\_2018.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf).

Though many of the efforts discussed above remain in early stages, we note that the Draft is aligned in some important ways with existing efforts. However, there are opportunities for NIST to improve the Draft's alignment in key areas and enhance US leadership in establishing IoT security guidance that is effective, meaningful, and appropriately targeted. For example, the EU's *Cybersecurity Act* requires that any certification scheme – including its planned IoT certification scheme – address end-of-life guidance, vulnerability management, and supply chain risk management – three areas we highlight above. By developing guidance in these areas, NIST can help ensure its baseline's alignment with EU guidelines, and influence alignment with the forthcoming certification scheme proposal. In addition, legislation currently proposed in both chambers of the US Congress – the *IoT Cybersecurity Improvement Act* (S. 734/H.R. 1668) – would require that the Federal Government adopt NIST-developed IoT security guidance that addresses, at minimum, secure development among other considerations; by incorporating SDLC guidance into its draft baseline per BSA's recommendations, NIST can ensure its alignment with this potential legislative mandate.

Securing the Internet of Things is one of the most pressing challenges we face in the cybersecurity arena, and BSA and its members are eager to work with NIST to encourage more robust security measures across the IoT industry. We hope our recommendations will support NIST's efforts to promote best practices for IoT security. Thank you for the opportunity to comment on this important matter.

Sincerely,



Tommy Ross  
Senior Director, Policy