ITI Promoting Innovation Worldwide

February 7, Friday, 2020

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000)
Gaithersburg, MD 20899-2000

Via email to: iotsecurity@nist.gov

Re: ITI Comment to 2nd DRAFT NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline

The Information Technology Industry Council (ITI) appreciates the opportunity to submit the following comments on Draft (2nd) NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline to the National Institute of Standards and Technology (NIST) (NISTIR 8259 or the "2nd Draft").

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity and Internet companies. ITI seeks policy solutions for the increasingly connected world powered by the continuous rise of emerging technologies such as Internet of Things (IoT). The growth of network-connected devices, systems, and services comprising Internet of Things (IoT) creates immense opportunities and benefits for our society. To realize the great benefits of connected devices while minimizing the potentially significant risks posed by malicious actors seeking to exploit them, these devices must be secure and resilient. Organizations and individuals increasingly face challenges in seeing and understanding cybersecurity risk across the full range of internet-connected devices, and some policymakers have disproportionately focused exclusively on IoT product security or other discrete parts of the ecosystem. ITI encourage stakeholders to take thoughtful, holistic approaches in managing risks to not only products but the various parts of networks and complex ecosystems that comprise global IoT security.

We encourage NIST to consider our overarching thematic comments, which can be summarized as follows:

- Continue to partner with industry on the Botnet Roadmap and facilitate international harmonization.
- Separate Foundational Activity and clarify the Core Baseline, *Table 1*, as the focal point of NISTIR 8259, preferably as a stand-alone document to reflect its weight and consensus.
- Send clear signals that NISTIR 8259 is not generally intended as a wholesale reference to be incorporated by regulators and that the baselines are voluntary best practices.

We further expand on these general comments immediately below, followed by more detailed line-by-line comments.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Overarching Comments

Continue to Partner with Industry and Facilitate Global Harmonization

The US Administration's Roadmap Toward Resilience Against Botnets (Botnet Roadmap)[1] and NIST's IoT work via NISTOR 8259 to advance core baseline capabilities were positive steps to forge greater collaboration between government, industry, and academics on IoT security. ITI co-founded the Council to Secure the Digital Economy (CSDE) which published an International Anti-Botnet Guide[2] to identify practices and capabilities for combating botnets and other automated threats (a document which was cited multiple times in the Botnet Roadmap), and we participated in the CSDE-driven C2 consensus with 20 other associations to coalesce around IoT device security baselines.[3] We welcome NIST's efforts to map the CSDE consensus in the 2nd Draft as well as other voluntary international references such as IEC, ESTI and ENISA. Moving forward, public- private partnerships will continue to be critical to identifying solutions to the many dimensions of the IoT security issue. We continue to encourage NIST and US Administration to work with industry across sectors on identifying consensus IoT security solutions, and additionally welcome continuing efforts to drive globally harmonized solutions via open, consensus-driven international standards to ensure global interoperability.

Separate Foundational Activity and Make the Core Baseline a Stand-alone Document

While we welcome that NIST has made improvements to the sections that go beyond the "Core Device Cybersecurity Capability Baseline for Securable IoT Devices" in the previous draft, we note that the underlying issue from the prior version of NISTIR 8259 remains. Although we appreciate NIST's well-intentioned effort to incorporate those sections (i.e. Foundational Activity) into the draft, inclusion of the additional sections as currently drafted may create confusion as to what parts of the document are considered as part of the consensus baseline, and what component parts are not. The "Core Baseline," *Table 1,* should be clearly identified and distinctly separated in the NISTIR 8259 to reflect its preeminent importance. Any confusion between the two concepts will unnecessarily dilute and negatively affect the impact of the "Core Baseline," as explained further below.

First, the "Core Baseline," *Table 1*, is included under the umbrella of "Foundational Activity," implying that the baseline capabilities are just one part of a set of foundational activities, blurring the distinction between the two terms and potentially downgrading the importance of the core baseline that NIST seeks to enshrine. The "Core Baseline" is unmistakably the focal point of NISTIR 8259 and should be clearly set apart as distinct from the rest of the discussion of "Foundational Activity." The core baseline is fundamentally more deeply grounded in consensus, and thus should be underscored and separated from the other "Foundational Activities" given that it relies upon and is aligned with the ongoing work of more than a dozen IoT device cybersecurity guidance documents published by standard-setting bodies, associations, and government agencies. The

[1] Commerce Dept. and Dept. of Homeland Security, A Roadmap Toward Resilience Against Botnets.
[2] CSDE, International Anti-Botnet Guide.
[3] CSDE, The C2 Consensus on IoT Device Security Baseline Capabilities.

other proposed "Foundational Activities" do not and cannot represent the same weight of consensus because they are a matter of ongoing discussion.

Second, subjugating the "Core Baseline" underneath "Foundational Activity" will weaken the impact of the "Core Baseline" in the marketplace and will implicitly give too much weight to activities, like communications to customers, which are not part of the "Core Baseline" consensus. Although the "Foundational Activities" in "Activity 6: Decide what to communicate to customers and how to communicate it" are now posed as a series of questions that manufacturers can answer, their inclusion as a "Foundational Activity" within a NIST document that includes the "Core Baseline" could still be misinterpreted – or even expropriated – by courts, regulators, and/or state legislatures as "baseline" mandates.

Finally, the blurring of lines and resulting confusion between "Foundational Activities" and "Core Baseline" categories will have practical implications. NIST should be aware that the conflation of these two terms may decrease the likelihood of manufacturers explicitly adopting and relying upon NISTIR 8259 for fear of inadvertently opening themselves to liability. For instance, if a manufacturer states that it is adopting NIST's approach, it will likely be unclear what this adoption entails. Does it mean the manufacturer has adopted the "Core Baseline"? Does it mean the manufacturer has committed to addressing the questions posed in the other "Foundational Activities?" We recommend that NIST clearly delineate the "Core Baseline" from the balance of the "Foundational Activities" articulated in NISTIR 8259, ideally as a stand-alone document which will most effectively convey the weight and strength of consensus underlying the baseline.

Send Clear Signals to Regulators on Purpose of "Core Baseline" and the broader NISTIR 8259

We welcome the increased attention by global policymakers on addressing IoT security issues. However, we observe that many policymakers are jumping to considering regulating IoT devices, including establishing certification requirements, while skipping over threshold issues such as identifying basic security practices or identifying the relevant international standards. Given that NISTIR 8259 pulls together a set of core baseline capabilities identified through global consensus, NIST should send a clear signal on the purpose of the document, underscoring that neither the "Core Baseline" nor "Foundational Activities" are intended to be appropriated as mandatory regulatory requirements.

At the same time, because we understand NIST will have limited control over how NISTIR 8259 is ultimately used, NIST should consider preparing for the document's potential use by a regulator, a policymaker, or a court. To avoid any confusion in this regard, NIST should try to do what it can to clarify that NISTIR 8259 is not intended as a reference to be "dropped in" wholesale to state or federal laws, as doing so can yield problematic results. It is not hypothetical that NISTIR 8259 may be placed within a state law or federal law as a mandatory requirement. For example, Ohio has made a decision to use NIST's Cybersecurity Framework as a safe harbor, with the Cybersecurity Framework listed as the "'framework for improving critical infrastructure cybersecurity developed by the national institute of standards and technology."[4] The Ohio law refers to the entire Cybersecurity Framework document, not a section or table from within the document. NIST should seek to minimize the likelihood of policymakers similarly referencing NISTIR 8259 wholesale in IoT security bills by addressing the blurred lines between "Foundational Activity" and the "Core

[4] Ohio Data Protection Act, SB220, 2018.

Baseline," as recommended above. The former is largely a discussion of issues a manufacturer could consider, while the latter is a baseline for IoT security based upon industry and government consensus.

NIST should emphasize that both the "Foundational Activity" and "Core Baseline" sections are proposed as voluntary, and not intended as mandatory requirements, given that adopting security practices is a constant process of improvement. Additionally, any distinct IoT security certification or requirement that varies significantly across individual U.S. states or foreign jurisdictions may fragment the global IoT security landscape by reducing the efficiencies of scale in solutions, development and consumer awareness.

Detailed Comments

The below list of detailed comments identified with line and page provides guidance and clarification on specific sections and language throughout the document. Please see the table below:

Section	Detailed Recommendations
Executive Summary Line 154	The document could be improved by better defining target audiences. ITI does not have the impression that the target audience is the consumer but because the document states that the "customer" must manage its security, and the document uses ETSI 103645 as a reference, which is dedicated to the consumer, NIST should clarify who the target audience is and is not.
Executive Summary Line 155	We would like to propose that NISTA adds additional language to clarify scope and audience due to the reasons below: While no simple internationally recognized definition of IoT currently exists, and it seems that NISTIR 8259 is intended to address a wide range of IoT devices, we would like to propose some additional language to clarify the scope of IoT devices covered in the document. ITI proposes below a slight clarification on the language clarifying the focus of NISTIR 8259 scope is finished, end products, not components. **Components of another device, such as a processor, are not able to function on their own in this context and should thus be considered as beyond the scope for NISTIR 8259.**
Additional comment on IoT Scope, Line 284-294, page 1	In addition to the above, to improve the clarity of the paragraph below we propose the following modifications: "The publication is intended to address a wide range of IoT devices. 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 beyond the scope for this publication.** Some IoT devices may be dependent on specific other devices (e.g., a hub) or systems (e.g., a cloud) for some functionality. IoT devices will be used in systems and environments with many other devices and components, some of which may be IoT devices, while others may be conventional IT equipment. All parts of the IoT ecosystem other than the IoT devices themselves are outside the scope of this publication."
Line 332 & 589, page 10	The sentence "Once a device is on the market, many cybersecurity changes may no longer be viable, especially if they necessitate changes to hardware, and those that can still be accomplished may be much more costly and difficult than if they had been done pre-market" should be further contextualized and refined to ensure it does not create confusion with respect to the ability of hardware-based solutions to support the capabilities in the *post-market stage*, or create a (mistaken) assumption that hardware cannot be changed or patched. Many solutions embedded in hardware, such as secure device onboarding and provisioning of devices (see comment on this topic) can be configured at the post-market stage and harden and support the security capabilities of IoT devices, in addition to software. Similarly, microcode or firmware-based code modifications can allow for *post-market* provisioning and configuration of hardware-based solutions in devices, in a manner that supports the capabilities (see also proposed modification for the definition of firmware). Proposed revisions: **Once a device is on the market, many cybersecurity changes may no longer be viable, and those that can still be accomplished may be more costly and difficult than if they had been done pre-market.**
Lines 372, 528, 694 & 957, page 4, 9, 15 & 23 Software and Firmware Update	With respect to the term "the ability to confirm the validity of any update before installing it" – consider changing the term "validity" to the term "authenticity." With respect to this sentence, "the ability to configure remote update mechanisms to be either automatically or manually initiated for update downloads and installations," since remote patching is not technically feasible in some architectures and cases, consider rewording to reflect that this capability is conditional upon the ability to perform remote updates. Proposed revisions: **The ability to configure remote update mechanisms to be either automatically or manually initiated for update downloads and installations, when remote update is feasible.**
Line 411	The Pre-market & Post-market activities described here are strongly related to the SDL (IEC 62443-4-1) process activities. We recommend referencing these

Section 3 Manufacturer Activities Impacting the IoT Device Pre-Market Phase	standards in the document (all the existing references are aiming to IEC 62443-4-2 Component Technical Capabilities). Increasing device security implicates the whole SDL process to create and provide Security Guidelines to the end-user (or the integrator / deployment service provider).
Line 674, Device Identification	In the explanatory notes (not as a proposed baseline capability) consider adding language to explain that in certain use cases and environments it may be desirable that the physical ID be immutable. In that regard, to enable stronger identification of devices during the process of authentication and provisioning, it is desirable the device Identifier would be both unique and immutable*, i.e.,* be stored in a way that protects it from modification.
Line 694, page 15 &30 Firmware Definition	The current proposed definition of "Firmware" may be outdated and is not technically accurate in the context of NISTIR 8259. It seems for the context of NISTIR 8259, the term firmware represents a more complex technical environment of microcode modifications than ROM hardware components. The following definition, for the context for NISTIR 8259, should be considered: Firmware: **"Firmware is a set of instructions programmed on hardware".**
Line 787 Section 4 Manufacturer Activities Impacting the IoT Device Post-Market Phase	The Pre-market & Post-market activities described here are strongly related to the SDL (IEC 62443-4-1) process activities. We recommend referencing these standards in the document (all the existing references are aiming to IEC 62443-4-2 Component Technical Capabilities). Increasing device security implicates the whole SDL process to create and provide Security Guidelines to the end-user (or the integrator / deployment service provider).
Lines 916-918, page 22 Device Configuration	With respect to the term "secure default," consider changing the term "secure default" to "secure restoration configuration," since the ability to reset can be to a secured restoration point (which may not necessarily be the "factory default," due to subsequent patching with anti-rollback requirements).
Line 979 & 686 Data Protection	"Data" (and "all data") in the context of the Data Protection capability does not necessarily contain PII, but may be limited to machine-to-machine data necessary for the operation of the device and performance of the capability. Thus the relation between this capability, the level of protection which depends on the nature of the data and "costumer," and existing privacy regulations could be clarified. **ITI proposes using the term "appropriate data," instead of "all data."**
Lines 686 Logical Access to Interfaces	The ability to logically restrict access to each network interface (e.g., device authentication, user authentication) could be reworded to "the ability to logically restrict network access to only authorized entities."

Lines 589, page 10	With respect to: "In addition to identifying suitable means for addressing each cybersecurity goal, manufacturers can also answer this question: how robustly must each technical means be implemented in order to achieve the cybersecurity goal? Here are some examples of potential robustness considerations: Whether it needs to be implemented in hardware *or can be implemented in software instead*" Manufacturers should be encouraged to implement layered security architecture with logical entity separation and isolation utilizing software, firmware *and* hardware solutions to harden the capabilities, not either/or. The term "instead" should be reconsidered, and software, firmware and hardware implementations should be encouraged in this context. Proposed language: **In addition to identifying suitable means for addressing each cybersecurity goal, manufacturers can also answer this question: how robustly must each technical means be implemented in order to achieve the cybersecurity goal? Here are some examples of potential robustness considerations: Whether the technical means can be implemented in multiple layers: hardware, firmware, and software.**
New proposed addition as a consideration (not as baseline): Domain Isolation	In highly sensitive IoT environments domain isolation might be an applicable capability that can support secure execution on IoT devices and a trusted application environment. Isolated enclaves or other means of domain isolation can support secure execution and transfer of sensitive data, processes, and keys at runtime.
New proposed addition as a consideration (not as baseline): Secure Onboarding of Devices (Late Binding), Post-Manufacturing and Pre-Manufacturing	Hardware and Software solutions can support automatic provisioning and configuration of authorized devices using mechanisms. Late binding of keys and other credentials can improve flexibility of application and local-site security for provisioning and configuration of IoT devices. Hardware-based solutions allow flexibility in provisioning, including in post-market stages.

ITI has been pleased to respond to this public comment, and we would like to reiterate our industry's commitment to promoting global and domestic harmonization of IoT security proposals consistent with core baseline capabilities for IoT security, driven by industry consensus, public-private collaboration and grounded in global standards. We look forward to continuing to work with NIST and other USG stakeholders to ensure IoT can maximize its benefits while mitigating risks using the best globally interoperable solutions.

Sincerely,

John Miller
Senior Vice President of Policy and Senior Counsel
Information Technology Industry Council