



April 14, 2018

Submitted electronically via NISTIR-8200@nist.gov

National Institute of Standards & Technology
Mr. Michael Hogan
Mr. Ben Piccarreta
100 Bureau Drive
Gaithersburg, MD 20899

RE: Request for Comments - NISTIR 8200
Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things¹

Dear Messrs. Hogan & Piccarreta,

In response to your request for comments, the Agelight Advisory Group submits the following comments. Agelight commends NIST's efforts to help address the risks and vulnerabilities inherent with the growing number of connected devices. We believe both the public and private sectors have a shared and collective responsibility to develop and embrace best practices, controls and standards to help protect users, critical infrastructure and the internet and society at-large from harm.

With the rapid pace of innovation and complexity of the IoT ecosystem, we encourage NIST to consider more broadly accepted best practices and policies which are proven to help protect users from harm and abuse of their data. The following is a summary of general comments including the rationale and proposed clarifications in one or more areas in your draft report.

1. **Relevant cybersecurity efforts.** We are requesting NIST to consider inclusion of the IoT Safety & Trust Design Architecture and Risk Toolkit®, (ISTA).² This is substantial multi-stakeholder effort which harmonizes and distils recommendations from organizations globally.³ Recognizing all standards and controls are not equal, the ISTA provides a risk tolerance assessment and management tool to help developers identify and prioritize development efforts. The utility is three-fold. First for industry and their development and engineering efforts, 2) to serve to assist in product selection and operation through a device life cycle for consumers and enterprise and 3) for retailers to evaluate products they merchandize.
2. **Device and consumer grade device definitions.** It is important to provide clarification regarding "consumer grade" devices used in the home, office and at play. The draft is silent to this distinction. While such devices are designed primarily for the consumer market, they are often found in the

¹ NISTIR 8200 (draft)

<https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf>

² ISTA v1.0 released April 11, 2018 <https://agelight.com/iot.html>

³ Summary of IoT standards best practices and recommended controls <https://agelight.com/IoTResources.html>

enterprise. Examples include smart TVs, thermostats, phone conferencing systems, smart coffee makers and related devices.⁴ These devices are unique from industrial controls and commercial grade devices yet run the same risk of introducing vulnerabilities and exploits to an organization's network infrastructure.

3. **Segmentation.** We encourage NIST to consider aligning efforts by industry to increase the utility and applicability. While many standards and principles may cover multiple segments, the context and importance of each may vary. Recommendations vary from industrial controls to medical, automotive to consumer grade devices. Benefits include providing more context, concise and actionable recommendations for the developer and device communities and reduce the risk of readers being overwhelmed by having to parse through irrelevant standards and controls.
4. **Device "hazardization"** is a key issue referring to the physical and/or life-safety risks when a device fails, yet the draft is somewhat silent to the scope and root causes from such hazards. It is recommended draft expand clarification to these risks. We define hazardization to include, not limited to the following use cases;
 - a. A loss or degradation of a product's safety features through a malfunction or a change in performance due to software updates
 - b. A loss of connectivity and a corresponding loss of function
 - c. The corruption of data used to support a safety feature
 - d. Potential physical harms from wearable and smart home and other devices
 - e. The risks of a device being orphaned, abandoned or "bricked" by the manufacturer
 - f. Vulnerabilities which hackers intentionally compromise with the intent to create physical safety risks. By targeting 1000's of devices simultaneously a coordinated attack could have a significant impact to critical infrastructure and society at-large.

It is suggested NIST collaborate with the Consumer Product Safety Commission and other agencies to reduce the risk of duplicating efforts and fragmenting industry guidelines and best practices.

5. **IoT privacy is a global issue,** transcending geographic borders. The draft while focused on security, needs to acknowledge the data privacy issues and associated risks. Many of the benefits realized from the use of IoT devices are enhanced and dependent on machine learning and artificial intelligence gathering of users' off-line lifestyle. When combined with online profiling and data analytics, the privacy implications are amplified. This creates an inherent conflict with data minimization principles. All too often users (in these cases consumers and businesses) are not fully aware or adequately informed of the extent of the ubiquitous data being collected and how and if they can control it.

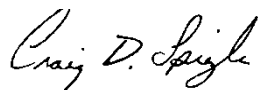
This underscores the importance of international coordination. Viewing privacy from a US perspective would be misguided and short sided. At a minimum it is suggested NIST consider the implications of GDPR regarding the disclosures and the respective collection, use, processing and storage of any user's data. As a reference the ISTA outlines several key compliance requirements.

⁴ Differences between industrial or enterprise grade and consumer grade devices vary greatly by manufacturer. These can span from warranties periods, support offerings (availability, duration) to device ruggedness, durability and level of testing and processor speeds.

6. **Device sustainability, lifecycle and end of life support** is a key issue in the ability to manage the deployment, operation and in some cases the revocation of a device. While there is no perfect security, safety or privacy, in theory devices should ship safe and be supported through their life. As highlighted by the NITA working group, patching and device security commitments should be disclosed prior to product purchase.⁵ As specified in the ISTA, mechanisms are needed communicate to the user of critical safety alerts including product recalls and end-of life communications.

I look forward to working with NIST and participating in future multi-stakeholder initiatives. Working together we can help society maximize the promise of IoT while helping to prevent and mitigate the security, privacy and safety issues we are faced with today. If you would like to discuss these comments in greater detail, please do not hesitate to call.

Respectively,



Craig D. Spiegle
Managing Director, AgeLight Advisory Group
Founder & Chairman Emeritus, Online Trust Alliance
<https://agelight.com/IoT.html>
+1 425-985-1421
@craigspi

⁵ NTIA multi-stakeholder initiative <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security>