Signify

April 17, 2019

via e-mail: jordan@isoc.org
pamela.miller@canada.ca
taylor.bentley@canada.ca

The Internet Society,
Chapter Canada

Attn: Katie Watson Jordan
Policy Advisor, North America
Internet Society

RE: SECURING THE INTERNET OF THINGS - A CANADIAN MULTISTAKEHOLDER PROCESS (DRAFT REPORT #5, DATED FEBRUARY 27, 2019)

Dear Mrs. Jordan

Signify appreciates the opportunity to provide the attached comments on the Draft Report on SECURING THE INTERNET OF THINGS - A CANADIAN MULTISTAKEHOLDER PROCESS.

Signify is the new company name of Philips Lighting. We are the world leader in lighting and provide our customers with high-quality, energy-efficient lighting products, systems and services. We turn light sources into points of data to connect more devices, places and people through light, contributing to a safer, more productive and smarter world.

The choice of our new company name originates from the fact that light becomes an intelligent language, which connects and conveys meaning.

Signify is the world leader in lighting for professionals, consumers and lighting for the Internet of Things (IoT). Our energy efficient lighting products, systems and services enable our customers to enjoy a superior quality of light, and make people’s lives safer and more comfortable, and businesses more productive and cities more livable.

We lead the industry in connected lighting systems and services, leveraging the Internet of Things (IoT) to take light beyond illumination and transform homes, buildings and urban spaces.

With 2018 sales of EUR 6.4 billion, approximately 29,000 employees and a presence in over 70 countries, we're unlocking the extraordinary potential of light for brighter lives and a better world.

Our detailed comments follow. We look forward to working with the Internet Society and to participate on Canadian Internet Governance Forums on this effort. If you require clarification about our comments please contact me directly or Harsha Banavara, our Cybersecurity Technical Policy Manager.

Sincerely,

Dejan Lenasi, P.Eng.,MSc.EE.
Technical Policy Manager
Standards and Regulations Canada
Signify North America Corporation
+ 1.778.386.9190
dejan.lenasi@signify.com

Harsha Banavara
Cybersecurity Technical Policy Manager
Standards & Regulations Americas
Signify North America Corporation
+ 1.615.540.7018
harsha.banavara@signify.com

Signify

SECURING THE INTERNET OF THINGS - A CANADIAN MULTISTAKEHOLDER PROCESS (DRAFT REPORT #5, DATED FEBRUARY 27, 2019)

Imagine in a diverse world with new 'things' getting connected to the internet increasing exponentially day by day, if we can all speak in one security language and have greater global alignment. We appreciate the efforts this group puts towards realizing that goal and the bottom-up process being followed throughout the Canadian Multistakeholder meetings involving all relevant stakeholders.

Signify has reviewed the draft outcomes report from the Canadian Multistakeholder Process and is pleased to provide the following comments:

Cybersecurity Standards

1. To help with a globalization, we suggest the reference (and practical use) to IEC standards rather than to local North American standards (e.g. UL or CSA).

   Ref. to the following sections.

2. While it is not claimed to include a comprehensive list of relevant global cybersecurity standards, missing of IEC 62443 suite of standards (global in scope) is notable. Though not all parts of this standard may be applicable to the scope of this Multistakeholder process, few parts such as 4-1 (Secure Development Lifecycle), 4-2 (Product requirements), 3-3 (System Requirements) should have been included as part of this report. Some of the other standards noted in this draft in turn refer IEC 62443 and aligns to the Multistakeholder process goal of harmonization.

3. Initially it appears no mandatory requirements are proposed for manufacturers. However, in Page 38 'Minimum attributes that a vendor should have regardless of product and service' is proposed. They align to ioXt security pledge; ETSI TS 103 645 and the UK IoT Consumer Code of Practice. However, no reference to ETSI has been attributed.

4. Staying on Page 38, while it is true that in order to have end-to-end security, people play a significant role and a knowledgeable buyer can make a well-informed decision to purchase a secure product, it appears the onus is on the buyer or at least the language used in this document suggest so. The challenge lies not in answering the aspects listed out in the document, but to ensure the buyer is knowledgeable enough that they understand security attributes that need to be considered for evaluating a product.

5. In Page 41, it is mentioned UL 2900 standard does not have any requirements for privacy. While that is true, it is also not applicable for 'cloud' part of a solution. For the sake of transparency this

statement should be included as well. In page 41, from a safety viewpoint only IEC 15208 is referenced; on this, we may have additional comment within the next 15 days.

6. In page 42, there is a specific reference made to Lighting with Security testing and evaluation to UL 2900 or equivalent made in the same sentence. As mentioned earlier, document misses the reference to the IEC 62443 having global scope and only called out currently US & Canada recognized UL 2900. Furthermore, it is to be noted that the UL 2900, similar to IEC 62443, has multiple parts and relevance of those part(s) be mentioned explicitly. E.g. HVAC – UL 2900-1 & UL 2900-2-2.

7. Later in Page 43, the report says, "If a vendor has one or both of these (ISO 27001 or ISO 9001) it should be regarded as a higher level of assurance to a product and that the necessary security controls have been deployed". While something is better than nothing, an organization being compliant to these standards need not necessarily mean the products they manufacture is secure as well. Such generic statements are best avoided and require more discussion.

8. There a few typos such as in Page 42 & 45, e.g. full proof instead of fool proof, that can be proof read and we are sure will be taken care in the final draft report to be published after the final Multistakeholder meeting.

Device Labeling and Trustmarks Working Group

We agree that Labeling and Trustmarks would be a step in the right direction for an IoT Device and help customers make informed decision not only while acquiring but also using and disposing.

a) For customers to understand/accept the label, the effective way should be a combination of first and last row of Table 5; pg.35.

The label should indicate:

I. CATEGORIES (such as per Table 4 (pg.32): to indicate Category level (1,2,3) within the coloured bar (similar to Fig.1 at pg.17)

and

II. QR code: We support the usage of QR Code and a "Live Label". The use of labels is currently prevalent in the privacy domain and mentioned in upcoming regulations such as EU Cybersecurity Act.

b) The label shall not have:

I. individual SDO marks (e.g. CSA, UL, ETL…). First there is a substantial number of different (SDO specific) logos that would and complexity for customers to recognize/link them with the IoT security & privacy. Preferably all should agree with unique Internet Security & privacy logo (TBD), something similar to Energy Star logo that is easy to associate with the intent

II. The label shall not have the list of product standards etc. as this is useless and confusing. Customer need not (and do not) recognize any of those. Similarly, the Energy Efficiency labels typically do not reference to compliance standards.

Certification
It is in the best interest of manufacturers and consumers alike to keep the requirements voluntary until there is greater acceptance in the community and implementation by the manufacturers. At a later point in time it can be made mandatory in steps, spread across a few years. Groups such as Internet Society, ISED, CANARIE, etc. should also work with the provincial and/or federal government during the formulation of any prospective regulation.

Finally, there must be either an annual or biennial review of the standards/regulations to ensure technological advancement and policies / regulations go hand in hand.

END OF COMMENTS