Feedback on

**Securing the Internet of Things: A Canadian Multistakeholder Process Draft Report; The Internet Society; February 27, 2019**

Overall impression

Key to make sure from the outset that the process, in true multistakeholder manner, is “run by the MSG” and supported by the OC. Currently, the introductory text gives the impression that the process is run by the OC with input from the MSG. I think that needs to change.

The report gives a good impression of the work done in the working groups, yet findings are fragmented across three work streams, and do not easily lead to conclusions and recommendations in its current form. Examples include:

- List of abbreviations is incomplete [for suggested additions, see annex “additional abbreviations”];
- Doubles of key references is different workstreams, yet not fully. Most references in NRWG are captured in Table 2. Key reference standards/recommendations and issuing organizations (page 25), but not all (for instance the ETSI Secure IoT recommendation). [Suggested way forward: establish one list of key reference standards/recommendations and issuing organizations, and refer to that one list from other places in the document];
- No comparable conclusions per workstream, difficult to comprehend for any outsider how the workstreams and their conclusions hang together [suggested way forward: ensure there are similar level conclusions on each of the three workstreams, and pull these in an overall “Conclusions & Recommendations” section at the end of the document, bringing it all together].

Furthermore, it would be useful to more explicitly present the findings within a wider framework that is clear on the context. The introduction starts with that, but it stops there. [suggested way forward: insert a Chapter “Introduction” (including a paragraph on “Background/state-of-the-art” and “problem description” after the “Executive Summary” and prior to diving in the description of the work done by the first workstream,.]

The Executive Summary, IMHO, should be a self-standing document that reflects what is said in the report itself. It should only contain facts that are further explained in the report itself, and provide the “full story” with logic from <problem definition.; <purpose of project year 1>; :<main findings/conclusions>; <main recommendation (still to be formulated at this point?)>.

Recommended way forward

Much of the content is in the document or has at least been discussed in one or more of the workshops, yet the current document requires IMHO a deep edit to

become more useful for the next phase. A team of two editors would probably work better than throwing it back to the workstream leaders at this point (one with governance/policy expertise, one with technical/business practice expertise would be a good combination). I would expect to see a report with the following outline:

- Executive Summary (self-standing, reflecting the content of the chapters);
- Content list;
- Introduction; (including background/state-of-the-art and problem statement/purpose)
- Workstream 1; NRWG
- Workstream 2; Labeling WG
- Workstream 3; CEWG
- Conclusions and recommendations (bringing together the recommendations per workstream and provide one single set of focused actions, with clear attribution to stakeholders)
- Annexes

And each workstream report would have a similar structure (not only in "paragraph headings", but also in terms of what is covered per paragraph:

- introduction; (including background/state-of-the-art and problem statement/purpose)
- Work done
- Conclusions drawn
- Recommendations and proposed next steps

In conclusion

Hope these suggestions are deemed useful as a way forward to get the most value out of all the good work done over the past year.

Best regards

Maarten Botterman

21 March 2019

===ANNEX===

Suggested additional abbreviations:

AESP: Association of Energy Services Professionals
BCP: best current practice
CASL: Canadian Anti-Spam Legislation
CATLs: CTIA Authorized test labs
CCPSA: Canada Consumer Product Safety Act

CEWG:Consumer Education Working Group
CIPPIC: Canadian Internet Policy and Public Interest Clinic
CIRA: Canadian Internet Registration Authority
CSA: Canadian Standards Association
CTIA: Cellular Telecommunications and Internet Association, USA
CVP: Cyber Verification Program
ISED: Ministry of Innovation Science and Economic Development
ISP: Internet Service Provider
MUD: Manufacturer Usage Description
NCCoE: National Cybersecurity Center of Excellence (part of NIST)
NIST: National Institute of Standards and Technology, USA
OSMUD: Open Source Manufacturer Usage Description @ osmud.org
OWASP: Open Web Application Security Project
PIPEDA: Personal Information Protection and Electronic Documents Act
SIDN: Stichting Internet Domain Namen (registry for .NL)
SPIN: Security and Privacy for In-home Networks by SIDN
UPnP: Universal Plug and Play