Feedback on "Securing the Internet of Things" Draft Report
From the Canadian Multistakeholder Process
dated February 27, 2019

Provided by: Jeff Wilbur, Technical Director, Online Trust Alliance of the Internet Society,
wilbur@isoc.org

The Online Trust Alliance, an initiative of the Internet Society, is pleased to provide feedback to the draft outcomes report from the Canadian Multistakeholder Process. This document is structured to address the items listed on iotsecurity2018.ca –

- Some level of agreement with the conclusions of the three working groups
- If you disagree with the conclusions of the three working groups, please give concrete information why
- Any additional resources that this group, and other Canadian stakeholders, should consider
- Your assessment of what conclusions should be prioritized as the main recommendations
- Your view of how the overall report should be framed in terms of audience, themes, Canada's role in the global conversation, or any other suggestions
- A willingness and capacity to contribute to this work going forward

Agreement with Working Groups

OTA generally agrees with the recommendations of the working groups and commends the efforts of each group to conduct research, articulate the issues being addressed by each group, and provide clear summary recommendations and next steps. We do have some additional comments on the various sections –

- **Executive Summary**
  - We recommend that the last sentence in the first paragraph under 1.3 be clarified regarding what is in scope and out of scope for IoT devices (this may come down to the word "support").
  - We also recommend that IoT "weaponization" be added to the end of the third paragraph in 1.3. It already addresses attacks on individuals but does not identify attacks by devices on the Internet at large, which is called out later in the report.
- **Device Labeling and Trustmarks Working Group**
  - It seems that privacy is in scope for these recommendations. It is called out in many areas, including as part of section 3.1, other referenced frameworks/guidelines, as number three of the eight minimum attributes listed on page 38, Tables 6 and 7, and as part of next steps in section 3.4. We recommend that if privacy is to be explicitly included in the guidelines and

associated labeling that it be stated as such up front. If the inclusion of privacy has not yet been determined, that should be clarified.
    - The focus on labeling seems to be focused exclusively on devices. Though it complicates the environment and any certification/testing, we recommend that reference is also made to the applications controlling the devices and the backend services supporting the devices. Maybe they go through their own labelling process or maybe they are included as part of the device assessment, but they are critical to the overall security and privacy capability of the solution, so need to be considered in some way.
    - In the "Determine Potential Labels" section on pages 42-43, OTA should be removed since there is not currently a labeling program based on OTA guidelines.
    - We wholeheartedly agree with the next steps that reference collaboration and tracking of other global IoT security and privacy initiatives. There are many efforts that are substantially similar and lining up on common goals can help create momentum and desired behavioral change more quickly.
- **Consumer Education Working Group**
    - The comment regarding inclusion of privacy made above applies to this group as well since it is referenced in the Recommendations in section 4.4.
    - Regarding the recommendations, it might be useful to break down the "supply side" roles into smaller pieces since the role of manufacturers, retailers and civil society can be very different in the way they participate in consumer awareness (e.g., manufacturers should clearly be the source of specific information regarding security and privacy, but retailers can package it more broadly to educate buyers and possibly differentiate products according to security and privacy characteristics, while civil society can do broad education campaigns and consumer advocacy to other stakeholders).
    - It seems that some elements of the scope of the CEWG are beyond the scope of the overall project (specifically the reference to vehicles and smart cities in section 4.3). While this may be perfectly appropriate for educating consumers it a world becoming more IoT-heavy every day, it should be clear how the scope of this working group relates to other working groups and the overall project scope.

Additional Resources to Consider

There are some existing references and new/additional resources and activities to consider –

- The reference to the "IoT Cybersecurity Improvement Act" should be updated to add "of 2019" and link to the updated bill that was reintroduced on March 11, 2019. https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019
- The reference to the UK Code of Practice from March 2018 in the middle of page 20 could be updated to reference the final report issued in October 2018 (which is also reference later in the report)

- The Australian efforts listed on pages 26, 27 and 28 have likely shifted and are now more aligned with the UK effort. We may be able to help connect appropriate parties to update this section to reflect the latest status.
- We recommend to consider adding NIST, ENISA, UK DCMS and ETSI to 3.4.a., though we recognize that the list was not intended to be exhaustive.
- Another labelling program that has recently been introduced is the Trustable Technology Mark (https://trustabletech.org/), a self-asserted mark covering broad aspects of IoT security and privacy
- NIST is in the midst of defining baseline IoT security recommendations, with conclusion expected by the fall of 2019. Draft guidelines are out for comment and can be found at https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf.
- Depending on how exhaustive the list of IoT regulatory/legislative efforts is intended to be, California has passed an IoT security law (https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327) and many other states have draft legislation. Most are geared toward minimum guidelines.
- The UK government is expected to release further research and their recommendations regarding labeling of IoT consumer devices by mid-2019.
- Another OTA resource to consider for Appendix VI is the OTA "Enterprise IoT Security Checklist", https://otalliance.org/system/files/files/initiative/documents/enterprise_iot_checklist.pdf.
- Another Internet Society resource to consider for Appendix VI is https://www.internetsociety.org/resources/doc/2018/top-tips-for-consumers-internet-of-things-security-and-privacy/

Prioritized Recommendations

- **Network Resilience Working Group**
    - We strongly recommend that the work done to create a threat list and framework for protecting IoT devices be promoted broadly to help others understand key threats and how to the address them.
    - The focus on practical implementation of MUD should also be continued and promoted to help provide guidance and proof of value to the industry.
- **Device Labeling and Trustmarks Working Group**
    - We wholeheartedly agree with the next steps that reference collaboration and tracking of other global IoT security and privacy initiatives. There are many efforts that are substantially similar and lining up on common goals can help create momentum and desired behavioral change more quickly.
    - We believe recommendation of a simple label with a live component is a good balance between quick visual indication and more in-depth education and real-time updates for consumers.

- **Consumer Education Working Group**
    - The recommendations in section 4.4 are strong, but messaging for consumers needs to be packaged in a way it can be easily digested (following learnings generated in next steps from section 4.3) and as mentioned earlier, we recommend that the supply side recommendations be tailored to specific supply side stakeholders.

Framing of Overall Report

- We believe the effort is well-framed overall in terms of scope, audiences, etc.
- Given the current global environment and sensitivity to IoT security and privacy, we believe it is important to address both security and privacy wherever possible.
- There are key stakeholders who can exert strong influence over each other, so addressing all of them – consumers, manufacturers, distribution channels and policymakers – is critical for success.
- We also believe it is critical to harmonize global efforts to streamline core guidelines for manufacturers, thus allowing them to move quickly and confidently to improve the security and privacy of their offerings. Recommendations for continued engagement in such efforts by the Canadian government help fulfill this goal.

Willingness and Capacity Going Forward

The OTA initiative of the Internet Society is willing to participate in this process going forward, primarily to provide guidance and advice.