CHC/IBC Joint CABA White Paper Proposal

Title: "IOT cyber security guidelines, standards and verification systems"

Currently there is not a recognized international IOT cybersecurity standard to which IOT device manufacturers can conform. This leaves manufactures without a label or customer facing recognition program that they can leverage to promote their cybersecurity credentials. Recognized organizations such as UL, CSA, Energy Star, ISO, OCF are working in this area but their approaches differ. Governments are now taking a role in promoting and developing standards, however legislation seems a few years away. Manufacturers are left scratching their heads wondering; where is this all heading and what can I do right now?
To complicate matters further IOT devices don't work in isolation, by their very nature they operate in a system that generally utilizes cloud based servers and multiple 3rd party service providers for connectivity and functionality. This widens the cybersecurity threat surfaces to way beyond just what comes in the box when you purchase a new IOT device.

This paper will look at the credible actors in this space and compare and contrast their approaches to cybersecurity verification, accreditation or testing.

Currently the list below outlines the range of options I am aware of, not all are appropriate to IOT cybersecurity, however they are related to this area.

- ISO 27001, 27032
- Canadian Standard Association- Cybersecurity Verification Process
- UL 2900-2-3 Cybersecurity Assurance Program
- Cloud security alliance
- Open Connectivity Foundation OCF 1.1.1 Security Specification
- ISO/IEC SC27
- ISO Standard 27002:2013
- OWASP Application Security Verification Standard 3.1
- Online Trust Alliance

The questions that I would like answering in the paper are-

What are the pros and cons of aligning with the different systems?
Which systems give a pass/fail/score vs just guidelines?
Which systems seem to be on a pathway to future product labelling ?
Who provides the greatest level of rigor?
What is more likely to be transformed in to a regulated standard?
What are the jurisdictional implications of these approaches?
What are the security gaps in each of the options ?
What are the Canadian and American government plans in this area?

Tim Mosley | Sr. Program Manager, Advanced DSM Strategies

BC Hydro
333 Dunsmuir St, 5th floor
Vancouver, BC V6B 5R3
E timothy.mosley@bchydro.com