Amsterdam, September 4 2015

To: Online trust alliance

Dear receiver,

We are hereby responding to your call for comments on the draft IoT trust framework. First of all we would like to thank you for taking this initiative. To enhance security and cyber resilience, we need open standards like the one you have drafted. We are also glad with the vendor-independent and open approach you have taken.

We have reviewed the standard with the team of ICT Institute. We are a boutique IT consulting firm active in Netherlands, UK and Belgium and have a network of IT experts who provide practical advice on software related management issues. Naturally, improving security is one of our clients' main concerns.

We have three main comments, described below.

1. Link requirements to cost / lifetime of devices

A practical problem with the standard is the one size fits all approach. One cannot make the same requirements for 100.000 euro cars as one can make for 2 euro toys. For independent makers of small devices, the standard is probably not feasible. A next version would probably benefit from having multiple levels.

2. Address source code transparency

Making the source code available is the best way to properly inform consumers on what devices are really doing and whether the security testing was effective. It is also important as many devices already contain open source software, and for these devices it is already mandatory for manufacturers to give access to the source code in some way. It would be good if the standard gave some practical advice on how manufacturers should do this.

3. Structure / cluster requirements

The current list is long and is perceived as unsorted. A suggested clustering into themes can be found here: http://ictinstitute.nl/ota-internet-of-things-security/

Best regards,

Sieuwert van Otterloo
sieuwert@ictinstitute.nl
+31 6 1050 9674 (mobile, central European time)