securebydesign@culture.gov.uk
Cyber Security Team,
Department for Digital, Culture, Media and Sport,
Level 4, 100 Parliament Street,
Westminster,
London, SW1A 2BQ

Date 25 April 2018
Reference Secure by Design: Improving the cyber security of consumer Internet of Things Report

Dear Sir/Madam,

On behalf of the Internet Society's European Regional Bureau and our UK Chapter [1], we are pleased to submit the following comments on the Department for Culture, Media & Sport's (DMCS) "Secure by Design: Improving the cyber security of consumer Internet of Things Report" ("the Report").

Security- and privacy-by-design are essential for the Internet of Things (IoT), and must be included in the design process from inception all the way through the formal end of life for a product. We are pleased to see the Report specifically address these extremely important issues:

- IoT vulnerabilities represent a threat not only to consumers, but to other services and the Internet itself by large scale attacks via insecure IoT devices
- The preference for the market to proactively solve this problem by delivering products and services with sufficient security and privacy incorporated from the start
- The need for global collaboration to address these issues, and for a shift in incentives to lead manufacturers to change their behaviour
- The guiding principles of the Report – reducing burden, increasing transparency and measurability, facilitating dialogue and resilience
- Beyond basic security and privacy norms, promoting a holistic and long-term view of the product lifecycle (e.g., implementation of a vulnerability disclosure policy, making systems resilient to outages, making it easy for consumers to delete personal data and making installation and maintenance of devices easy)
- Clearly delineating which Code of Conduct recommendations apply to which key stakeholders

We also would like to direct your attention to some key pieces of work we have developed in this area, that can serve as either a foundation or model for similar or complementary efforts to improve security-by-design and privacy-by-design. The Online Trust Alliance (OTA) [2] became part of the Internet Society in 2017, and is now run as an Internet Society initiative. The OTA "IoT Security & Privacy Trust Framework" [3] (an earlier version of which is referenced in your "Summary literature review of industry recommendations and international developments on IoT security"), contains a set of 40 principles reflecting input from more than 100 stakeholders, most of which are reflected in your Section 4 "Code of Practice".

There are a few additional principles that we would recommend be incorporated into the Code of Conduct, such as:

- Recovery mechanisms for user authentication,
- Resilience to brute force password attacks, and
- Disclosure of the manufacturer's data retention policy.

As noted, we see strong alignment in our approaches and core principles, and therefore would like to engage in further discussions to fully explore the synergies and determine whether additional Code of Conduct refinements are warranted.

We also believe we can be of assistance with a number of the supporting actions identified in Section 5. As part of the Internet Society's "IoT Trust by Design" efforts, we are engaged globally with policymakers, civil society, manufacturers and consumer testing organizations to raise the level of awareness about security and privacy in IoT products and services and what can be done to improve it.

For example, we at the Internet Society are engaged with a number of organizations exploring or developing consumer information approaches, labelling schemes and ways to better share consumer information. In addition, note the Internet Society's recently released policy brief "IoT Security for Policymakers" [4] which, as its title suggests, provides guidance and recommendations for policymakers and regulators as they pursue policy and regulatory options to improve IoT security and privacy-by-design (5.19).

We laud your goal that industry takes appropriate actions on its own to ensure the security of IoT devices. ISOC's Online Trust Alliance IoT initiative is one such action, which has helped industry to collaborate and take the lead in producing actionable privacy and security recommendations. As policy makers continue to explore ways to address the significant challenges presented by IoT devices, we would encourage you to, first, take into consideration such steps that industry has already taken and to support and promote such self-regulatory action (where appropriate, and in consultation with industry and other stakeholders). Second, given the cross-border nature of many IoT products and related services, we recommend that any exploration you undertake of IoT-related regulatory and enforcement measures be done through a process including industry and other relevant stakeholders, aimed at identifying cross-border and jurisdictional issues.

We are eager to remain engaged with you on all of these matters since we view this work as vitally important. We believe a multi-stakeholder approach is the right way to proceed, is consistent with our experience, and is the best way to achieve these goals in a very complex and fast-moving environment.

Sincerely,

Olivier Crépin-Leblond, President, Internet Society UK Chapter
Frédéric Donck, Internet Society Regional Bureau Director for Europe

[1] For more information about us, see

http://isoc-e.org/
https://www.internetsociety.org/about-internet-society/

https://www.internetsociety.org/iot/

[2] https://otalliance.org/

[3] https://otalliance.org/initiatives/internet-things

[4] https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/