Response to Request for Input on the Report and Code of Practice –

Secure by Design:
Improving the Cyber Security of Consumer Internet of Things Report

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

Submitted to securebydesign@culture.gov.uk (25th April 2018 deadline)

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Overall Comments on the Code of Practice

1. The UK Computing Research Committee broadly welcomes the proposed scope and content covered in the Code of Practice.

2. We would, however, recommend that they are reviewed every 2 years at a minimum. Threats change and defences will emerge from the public-private initiatives that are a key strength of the proposals.

3. We are concerned that the Code of Practice will be ineffective. The report refers to "the (IoT) market" (p.5). The use of this phrase belies the complex and diverse IoT **markets** (plural). Retailers and developers of, for instance, IoT televisions are not directly in competition with controllers for domestic heating systems. The adoption of the Code is jeopardised because most suppliers are overseas and supply chains are global. The UK market, although, growing, is not driving these developments.

4. Market forces are unlikely to lead to effective self-regulation in IoT devices. The report explicitly identifies the technical grounds for more active government intervention, referenced in introductory textbooks on market Economics[1]:

- Imperfect information – competition fails when consumers lack the information to make accurate and informed choices;

[1] See for instance http://www.econport.org/content/handbook/Market-Failure/Imperfect-Information/Dealing-with-Imperfect-Information.html

- Third party effects – competition and market forces fail to prevent third party effects where consumers are injured by good that they did not themselves purchase (see comments in the report on the Mirai bot nets).

5. The Code seems weaker than other comparable markings. The CE (European) and FCC (US) consumer markings governing electromagnetic interference provide evidence that individual devices are robust against interference and do not themselves emit electromagnetic interference. To display these markings, all devices sold in the US/UK have to be tested using standardised tests in accredited labs. We anticipate that the potential failure of the Code may lead to a similar scheme being introduced for IoT devices. It should be noted, however, that the CE/FCC markings provide no assurance about the safe or secure functionality of complex software-based systems.

6. The Code of Practice is silent on software quality and assurance; this is inconsistent with the detail in other areas. The UK research community is actively involved in advanced attack techniques, for instance, in the use of Machine Learning to direct automated fuzz testing. These methods have exposed significant security vulnerabilities in consumer products that were the result not of poor cyber security policies but through low quality software engineering practices.

7. The Code ignores the supply chain complexities of products that rely on components for which the vendor or manufacturer have no control – in terms of the firmware, for example, used by third parties.

8. We have some minor concerns over the ordering of the items in the Code – given that the recommendations are in priority order. For instance, the threats covered in item 13, including but not limited to buffer overflow attacks, arguably deserve greater attention.

9. As a research community we recognise the technical challenges in meeting the requirements in the Code. The wider report makes reference to maintaining minimum functionality during an update; for example to ensure heating or the provision of other potentially critical services. This is likely to have a profound impact on the user if they cannot anticipate or control the timing of these updates. If the Code were implemented as it stands the impact could be profound on quality of IoT services;

10. The rules on personal data mirror GDPR (as they should). However, they again raise significant practical, technical challenges. Will device manufacturers provide consumers with a free copy of all the data that a device has collected about them every time they ask for it? Similar concerns arise for the deletion of data on IoT devices developed overseas or marketed by third parties. The Code would seem to require uneconomic actions or a radical change to existing business models.

11. Points 9 and 10 in our response rest on the assumption that a Government supported Code is "reasonably practicable" to adopt. Without this it will be hard to sustain or, eventually, to enforce.

Detailed Comments on the 'Secure by Design' Report

A. Page 5: see comment 3 on the Code of Practice – we do not believe that there is any single IoT Market but a series of international, interconnected supply chains providing Internet enabled services across many different consumer products.

B. Page 7, Paragraph 1.8, there should also be a focus on national impact extending beyond domestic IoT devices to wider consumer products (jncluding connected vehicles with reference to the recent DfT principles) and IIoT services.

C. Page 8. 1.9, In the medium term we feel that more could be done by working with the vendors of domestic routers and gateways promoting enhanced security (scanning, monitoring, routing) for IoT domestic networks; as a market driven approach to a key component in consumer networks.

D. Page 23, 4.10 – greater emphasis should be placed on the requirement to ensure that the software update process is not itself the mechanism for cross-infection.

E. Page 27, 5.12 – including secure disposal in the list of considerations.