

Press release: Plans announced to introduce new laws for internet connected devices

- Basic cyber security features to be built into products
- Consumers will get better information on how secure their devices are
- Consultation now launched ahead of potential legislation

Plans to ensure that millions of household items that are connected to the internet are better protected from cyber attacks have been launched by Digital Minister Margot James.

Options that the Government will be consulting on include a mandatory new labelling scheme. The label would tell consumers how secure their products such as 'smart' TVs, toys and appliances are. The move means that retailers will only be able to sell products with an Internet of Things (IoT) security label.

The Government will be consulting on options including a mandatory new labelling scheme. The label would tell consumers how secure their products such as 'smart' TVs, toys and appliances are. The move means retailers will only be able to sell items with an Internet of Things (IoT) security label.

The consultation focuses on mandating the top three security requirements that are set out in the current 'Secure by Design' code of practice. These include that:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers explicitly state the minimum length of time for which the device will receive security updates through an end of life policy.

Following the consultation, the security label will initially be launched as a voluntary scheme to help consumers identify products that have basic security features and those that don't.

Digital Minister Margot James said:

Many consumer products that are connected to the internet are often found to be insecure, putting consumers privacy and security at risk. Our Code of Practice was the first step towards making sure that products have security features built in from the design stage and not bolted on as an afterthought.

These new proposals will help to improve the safety of Internet connected devices and is another milestone in our bid to be a

global leader in online safety.

National Cyber Security Centre (NCSC) Technical Director, Dr Ian Levy said:

Serious security problems in consumer IoT devices, such as pre-set unchangeable passwords, continue to be discovered and it's unacceptable that these are not being fixed by manufacturers.

This innovative labelling scheme is good news for consumers, empowering them to make informed decisions about the technology they are bringing into their homes.

CEO of techUK Julian David said:

techUK welcomes the publication of the Government's consultation on regulatory next steps for consumer IoT. This follows the Government's voluntary Secure by Design Code of Practice for consumer IoT security launched last year, which techUK supported. The Code advocates for stronger cyber security measures to be built into smart products right from the design stage.

We are pleased that the security requirements outlined in the consultation are consistent with the Secure by Design Code of Practice and key industry standards that already exist for consumer IoT devices. This is an important first step in creating flexible and purposeful regulation that stamps out poor security practices, which [techUK's research](#) shows can act as significant barriers on the take-up of consumer IoT devices.

The proposals set out have the potential to positively impact the security of devices made across the world and it is good to see the Government is working with international partners to ensure a consistent approach to IoT security. techUK looks forward to responding to this consultation on behalf of our members.

The consultation follows the government's voluntary Secure by Design Code of Practice for consumer IoT security launched last year. The Code advocates for stronger cyber security measures to be built into smart products right from the design stage, and has already been backed by Centrica Hive, HP Inc Geo and more recently Panasonic.

The proposals come a day after Margot James held a roundtable on IoT security with global technology companies. As a result Amazon, Philips, Panasonic, Samsung, Miele, Yale and Legrand affirmed their commitment to taking steps to ensure that effective security solutions are being implemented across IoT products on the market.

The Government is working with international partners to ensure that the

guidelines drive a consistent approach to IoT security. The proposals set out in the consultation have the potential to impact security of devices made across the world to meet the UK's future standards.

Alternative options to the label that Government are also consulting on would be to mandate retailers to not sell any products that do not adhere to the top three security requirements of the Code.

ENDS

Notes to editors:

The consultation document will be available on the Government's [Secure by Design](#) pages and is open for 5 weeks. It has been published alongside a consumer survey report which tested various label designs with 6,482 UK consumers as part of helping to create a labelling scheme that was backed by evidence.

The public consultation is part of a wider evidence based approach, to create regulatory proposals for consumer IoT products.

In February, ETSI, the European Standards Organisation, launched Technical Specification 103 645, the first globally-applicable industry standard on the cybersecurity of internet-connected consumer devices. TS 103 645 builds on the Code of Practice for Consumer IoT Security, but has been developed for wider European and global needs. [Cybersecurity Tech Accord signatories](#) endorsed the ETSI TS 103 645 in March 2019.

Stakeholders can submit feedback to the consultation via securebydesign@culture.gov.uk

The UK Government has also updated its guidance for consumers ('Smart devices: using them safely in your home') – the guidance has been published on DCMS and NCSC's website.

[The Industrial Strategy](#) sets out a long term plan to boost the productivity and earning power of people throughout the UK. It sets out how we are building a Britain fit for the future – how we will help businesses create better, higher-paying jobs in every part of the UK with investment in skills, industries and infrastructure.

The Minister made the announcement at the PETRAS/IET Living in the Internet of Things Conference (1-2 May 2019), at the Institution of Engineering and Technology, Savoy Place.