



Royalty-free stock vector ID: 1141257410

Apr 21, 2021 18:49 BST

## UK government announces plans for new IoT security law

Today, the UK government's Department for Digital, Culture, Media and Sport (DCMS) has published its [response](#) to its call for evidence seeking feedback on proposals to regulate the cyber security of consumer smart products.

A new law, which will likely be announced next month in the Queen's Speech, will require manufacturers to make sure that all consumer connected products meet minimum cyber security requirements before they are placed on the UK market. The law will also require them to publish a declaration of conformity, which should be verified by retailers.

These basic security requirements include:

- **Security updates:** according to plans set out in the Policy Paper, makers of smart devices including phones, speakers, and doorbells will now need to inform consumers about how long their devices will be protected through security updates upfront.
- **A ban on universal default passwords:** research, including our own with consumer champion, Which?, has repeatedly discovered a range of widely available connected devices which have been given easily guessable default passwords, such as 'password' or 'admin'. To tackle this, the new law will enforce a ban on manufacturers using default passwords.
- **Public point of contact for vulnerability reporting:** as well as placing a ban on using default passwords, the law will also require manufacturers to provide a public point of contact for anyone to report a vulnerability.

To bridge global efforts, the legislation is due to be interoperable and compatible with other product regulations and international standards.

This news comes as the number of connected devices continue to proliferate, with almost half (49%) of UK residents purchasing at least one smart device since the start of the coronavirus pandemic.

NCC Group's Hardware & Embedded systems practice has over the last five years researched heavily into the IoT space to uncover the security issues that continue to proliferate across the connected devices market in both the consume and enterprise sphere.

This includes working closely with UK consumer champion, Which?, to understand and expose the scope of issues, and to bring to the fore the impact of these weaknesses if compromised.

Last year, we were also named an Authorized Lab by the ioXt Alliance, the Global Standard for IoT Security and the industry group dedicated to building confidence in IoT products through multi-stakeholder security and privacy requirements, product compliance programmes, and public transparency.

**Commenting on the proposed legislation, Ollie Whitehouse, global CTO at**

**NCC Group said:** "For many years now we, alongside other campaigners and leaders across the cyber security industry, have been calling for a legislation that sets a clear benchmark for the security of connected devices.

"The proposals set out today mark a significant turning point for IoT security for the journey ahead of us. It's promising to see the emphasis placed on international engagement and the role the UK can play in shaping and setting global standards. We're also pleased to see that manufacturers are being encouraged to work towards compliance ahead of the law coming into force, which means that they should be given enough grace time to implement measures before they become a legal requirement.

"Looking ahead though, more detail on how this new law will be enforced is needed, including the body that will be responsible for spearheading the legislation. When this is decided, the enforcement body will need to have mandate, and non-compliance must have consequences to ensure that standards are set and met across the connected devices ecosystem. In turn, this will help to raise the cyber resilience of devices consumers and businesses use every day, and root out insecure devices in the UK market, and in due course, globally.

"That said, we do recognise that that this needs to be done in a way that allows a flexible and agile response to technological, international and threat actor evolution, which will require continuous monitoring, evaluation and evolution to respond to trends based on evidence."

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant

market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts



### **NCC Group Press Office**

Press Contact

All media enquires relating to NCC Group plc

[press@nccgroup.com](mailto:press@nccgroup.com)

+44 7824 412 405

+44 7976 234 970