BTHA 30 Second update – Cybersecurity Legislation

23rd April 2021

Introduction

The UK Government is pro-tech and values the benefits that technology and greater connectedness can bring. The innovations that have allowed an increasingly diverse range of consumer products to connect to the internet are no exception to this.

As part of their work to make the UK the safest place to be online, the UK Government have to be able to assure consumers that the devices being brought into their homes are secure - technological advancement cannot be at the expense of consumer security.

A call for views on regulatory proposals was launched in July 2020. The government's response to the call for views and further details of the world-leading legislative framework that they are been developing has now been announced. This represents a key milestone in being able to harness the opportunities presented by connected products, safe in the knowledge that this isn't at the expense of security.

https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation

Next Steps

Now that internationally accepted standards are in place, the government believes that the time has come to start to enforce these standards. The government will now legislate, when parliamentary time allows, to create a new robust scheme of regulation to protect consumers from insecure connected products. An enforcement body will be equipped with powers to investigate allegations of non-compliance and to take steps to ensure compliance. Following royal assent, the government will provide relevant economic actors with an **appropriate grace period** to adjust their business practices before the intended legislation fully comes into force.

Objectives

- Protect citizens, networks and infrastructure from harm
- Enabling emerging tech to grow and flourish by improving security, and Increasing consumer confidence
- Adopting a proportionate approach to placing obligations on relevant economic actors, without compromising effectiveness
- Continuing to protect citizens, networks and infrastructures from harm in the face of an uncertain future

Twelve key policy positions

1 - Defining products in scope	2 - Exempted product classes
The intended legislation will apply to any **network-connectable devices and their associated services** that are made **available primarily to consumers**, except products that are designated as out of scope.	Specific product classes that would otherwise fall within the scope of this legislation, but for which it would be inappropriate for it to apply to, will be **exempted from the legislative framework.**
3 - Adaptable scope	**4 - Interoperability**
Where changes to the wider regulatory, technological, or threat landscapes render it appropriate, the intended legislation will allow Ministers, subject to agreement by Parliament, to **adjust the scope of consumer connected products covered by this regulation** by updating the list of specific product classes exempted from its effects.	The government will ensure that the intended legislation is **interoperable with other existing or planned government interventions** covering contiguous, or overlapping product classes, such as BEIS commitments to regulate smart appliances.
5 - Obligations on economic actors	**6 - Security Requirements**
The legislation will place **proportionate obligations on relevant economic actors** involved in the transmission of in scope products to consumers to ensure that insecure products are not made available to UK consumers.	The legislation will obligate relevant economic actors to not make consumer connected products available on the UK market unless they **comply with certain security requirements, or designated standards.**
7 - Adaptable security requirements	**8 - Product Assurance**
Where changes to the wider regulatory, technological, or threat landscapes render it appropriate, the intended legislation will allow Ministers to **update the security requirements and designated standards** that relevant economic actors must ensure products made available on the UK market comply with.	Where changes to the wider technological or threat landscapes render it appropriate, the intended legislation will enable Ministers to **mandate product assurance**for particular categories of consumer connected products.
9 - Enforcement authority	**10 - Enforcement role and responsibilities**
An enforcement authority will investigate non-compliance, take action in relation to any non-compliance, and provide support to relevant economic actors to enable them to comply with their obligations.	To enable **proportionate enforcement across a range of contexts**, the legislation will equip the enforcement authority with **necessary powers**, as well as the ability to issue **appropriate corrective measures, sanctions** and potentially in the most serious circumstances, to bring forward criminal proceedings.
11 - Appeals	**12 - Proportionate transitional provisions**
Relevant economic actors will have the right to **appeal any sanctions or corrective measures** brought against them, in a manner consistent with the processes used in existing before the intended legislation fully product safety legislation.	Following royal assent, the government will provide relevant economic actors with an **appropriate grace period** to adjust their business practices comes into force.

Policy 1 - Products in Scope

- Includes only products that are intended to be used by consumers, or products that are likely to be used by consumers in reasonably foreseeable conditions, and excludes products that are only used by businesses or in industrial settings (although

products that are primarily used by consumers, but can also be used in a business environment, such as Smart TV's or connected security cameras, would be included)
- Includes only products that have a network interface (e.g. can communicate data via Wifi, Bluetooth, data cable etc.)
- Includes both devices and their associated services (where "product" is understood to refer to both of these). Some of our security requirements will apply to only the device, some apply to both the device and associated services. Associated services would not include 3rd party apps that may also run on the device (e.g. Netflix on a smart TV).
- Includes "ancillary" products that connect primarily to other devices

Non-exhaustive list of products within the scope of the intended regulation

- Smartphones
- Connected cameras, TVs and speakers
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Internet of Things base stations and hubs to which multiple devices connect
- Wearable connected fitness trackers
- Outdoor leisure products, such as handheld connected GPS devices that are not wearables
- Connected home automation and alarm systems
- Connected appliances, such as washing machines and fridges
- Smart home assistants

Policy 6 - Security Requirements

The legislation will obligate relevant economic actors to not make consumer connected products available on the UK market unless they **comply with certain security requirements, or designated standards.**

They intend to create two routes to conformity within the intended legislative framework:

1. The first route is to implement the security requirements as detailed in legislation. These initial security requirements have been derived from and align with the top three guidelines from the Code of Practice for Consumer IoT Security, and key provisions within ETSI European Standard (EN) 303 645.
2. As a second alternate route to conformity, we intend to designate relevant standards that can be implemented in lieu of the security requirements in legislation. Specific provisions/clauses of standards will be designated so that implementation of these achieves the same (or nearly the same) as implementation of the security requirements. This will enable us to facilitate alignment across jurisdictions.

Summary of security requirements and designated standards

Security Requirement	Explanation of intent	Designated external standards
Security Requirement 1 Ban universal default passwords	Our intent is to cover all passwords within the device, including those not normally accessible by the user, such as passwords on administrative interfaces, or within firmware of sub-components. Pre-installed software applications (Apps), including those that are 3rd party provided but pre-installed on a device, are also in scope. Our intent is also to ban passwords which may be unique per device, but are still easily guessable and therefore still present a risk (for example, if incremental counters are used such as 'password1', 'password2' and so on).	EN 303 645 provisions 5.1-1 and 5.1-2
Security Requirement 2 Implement a means to manage reports of vulnerabilities	The intent of this requirement is to provide a transparent route for third parties to report vulnerabilities to the manufacturer, making it possible for security issues to be resolved. This practice remains uncommon for manufacturers of consumer connected products, however, this is an essential mechanism to identify and address security shortcomings, and to aid security innovation in the sector. **Note: designated standards for this outcome must be applied to the device and associated digital services**	EN 303 645 provisions 5.2-1 **OR** ISO/IEC 29147(2018): clause 6.2
Security Requirement 3 Provide transparency on for how long, at a minimum, the product will receive security updates	Providing security updates is one of the most important mechanisms to protect consumers. Their purpose is to address security shortcomings that place consumer's privacy, data and security at risk and that are typically only identified, and able to be utilised, once the product is on the market. They also enable consumers to make better informed purchasing decisions. When buying a product, consumers need to be able to find out the minimum period of time for which that product will be supported with security updates. It should also be noted that the defined support period can always be extended unilaterally by the manufacturer.	EN 303 645 provision 5.3-13

Policy 7 – Adaptable security requirements

It may be necessary to introduce requirements in the future relating to (but not limited to) areas such as the following:

- User authentication
- Vulnerability reporting
- Software updates
- Protection of data at rest and in transit
- Security design principles for software and hardware
- Protection of personal data (privacy)

- Product and wider network resilience
- Provisions of information and guidance to product users

Policy 8 - Product Assurance

Some responses to the call for views highlighted the importance of product assurance service in achieving good security outcomes. They recognise this and strongly encourage voluntary take-up of assurance services for consumer connected products. In the future, it may be appropriate to require certain categories of consumer connected products, especially where the risk to consumers is considered to be high, to undergo an assurance process (for example independent assessment or assisted self-assessment).

For that reason, the intended legislation will enable Ministers to be able to mandate assurance for designated categories of consumer connected products. We do not have the intention to make use of this power at an initial stage, and would only do so following engagement with industry and analysis of benefits and costs.

However for members that want this service IASME has a voluntary assurance scheme. The IoT Security Assured scheme will be open to start ups and smaller companies to certify their smart products and reassure consumers they meet the required security standards. Devices that are certified to the IoT Security Assured scheme will display a logo to reassure consumers that their device meets these basic security requirements.

There is also likely to be a connected toys assurance scheme launched during the year and prior to the end of the transition period of the children's code.