Department for
Digital, Culture,
Media & Sport

MANDATING SECURITY REQUIREMENTS FOR CONSUMER 'IoT' PRODUCTS

Consultation Stage Impact Assessment

May 2019

Title: Mandating security requirements for consumer Internet of Things (IoT) products

Lead department or agency: Department for Digital, Culture, Media and Sport

Impact Assessment (IA)

Date: 01/05/2019

Stage: Consultation

Source of intervention: Domestic

Type of measure: Primary legislation

Contact for enquiries: evidence@culture.gov.uk

Summary: Intervention and Options

RPC Opinion: N/A

Cost of Preferred (or more likely) Option

Total Net Present Value	**Business Net Present Value**	**Net cost to business per year** (EANDCB in 2017 prices)	**Business Impact Target Status**
£298.6m	-£1m	£0.1m	Qualifying Regulatory Provision

What is the problem under consideration? Why is government intervention necessary?

Many consumer internet-connected devices, such as smart TVs and smart speakers, lack basic cyber security provisions. The rapid proliferation of these devices and lack of transparent information available means that consumer security, privacy and safety is being compromised. The wider economy also faces an increasing threat of large scale cyber-attacks through exploiting insecure consumer IoT devices. Recommended security requirements are often implemented by manufacturers as an afterthought, if at all, rather than during the design process. By mandating security labels on consumer IoT products, consumers will be able to make more informed purchasing decisions that lead to fewer insecure products on the market.

What are the policy objectives and the intended effects?

The policy objectives are to mandate the adoption of a security label for manufacturers of consumer IoT products. The outcome of this is for consumers to be informed about the security of the IoT products that they purchase. Through the label, consumers will be aware of security features of IoT devices and take this information into account to allow them to make informed

purchasing decisions. We envisage that changes in consumer behaviour, due to the label, will incentivise manufacturers to make devices secure by design (secondary effect), resulting in better protection of people's privacy, online security and safety. This approach will also help to mitigate the risk of DDoS (denial-of-service) attacks that are caused by exploitation of insecure consumer IoT devices.

What policy options have been considered, including any alternatives to regulation?

- Option 0: Do nothing (i.e. no regulation). Manufacturers can choose whether to implement the UK Government's voluntary label or voluntarily pledge to implement the Code of Practice guidelines.

We have considered the following regulatory options:

- Option A: Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self assess and implement a security label on their consumer IoT products. (Preferred option)
- Option B: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with manufacturers to self assess that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security.
- Option C: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers to self assess and to ensure that the label is on the appropriate product packaging.

Other options that have been considered:

- Option D: Adopt a potential consumer IoT certification scheme that may emerge from the EU cyber security certification framework being established by the EU Cybersecurity Act

Will the policy be reviewed? DCMS will periodically review the Code of Practice every two years. **If applicable, set review date:** next review date will be in October 2020.

Does implementation go beyond minimum EU requirements?		Yes		
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** **N/A**	**Non-traded:** **N/A**	

Summary: Analysis & Evidence Policy Option A

Description: Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self assess and implement a security label on their consumer IoT products.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low:	High:	Best Estimate:
2017	2022	10	15.4	907.6	361.9

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	0.3		Currently un-monetised	**0.3**
High	2.8		Currently un-monetised	**2.8**
Best Estimate	1.2		Currently un-monetised	**1.2**

Description and scale of key monetised costs by 'main affected groups'

The regulation would mandate manufacturers and retailers to produce and sell consumer IoT products display a positive or negative cyber security label on their packaging. This would allow consumers to identify whether the product complies with the top three guidelines of the Code of Practice. Costs to businesses would include familiarisation and self assessment costs associated with implementing the label. There will also be costs associated with redesigning product packaging to include the mandated label. DCMS has estimated that there are approximately 69 consumer IoT manufacturers in the UK.

Other key non-monetised costs by 'main affected groups'

As consumers become more informed through the mandatory label, manufacturers who produce products containing a "negative" label would likely incur reputational damage, which could result in lower sales leading to lower profits. Businesses may also incur indirect costs associated with improving their products in order to display a "positive" label. This cost is expected to be ongoing, however, it is assumed that businesses will only undertake voluntary improvements where the cost of doing so does not outweigh the benefits.

Other non-monetised costs include the cost to government of monitoring consumer IoT products to ensure that they are compliant by displaying a label, and the cost to retailers of inspecting their incoming stock. DCMS is carrying out research in order to be able to estimate these costs.

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)

Low	0		2.2	**18.2**
High	0		108.5	**907.9**
Best Estimate	0		43.4	**363.1**

Description and scale of key monetised benefits by 'main affected groups'

It is expected that the main benefits of labelling will accrue from a reduction in the number of insecure devices purchased by consumers, as well as secondary benefits of security improvements in consumer IoT products. This should result in a reduction in the number of breaches that consumers experience.

Other key non-monetised benefits by 'main affected groups'

Selling products with an IoT security label will allow consumers to make better informed purchasing decisions, with the assumption that companies whose products have positive labels will benefit from higher sales compared to competitors whose products have a negative label, resulting in higher profits. The label will increase consumer's security awareness and may encourage consumers to take action to secure their existing products, leading to lower costs associated with breaches. There is also a significant potential benefit to wider society of having fewer insecure IoT devices on the market open to hacking and use in wide-scale DDoS attacks.

Key assumptions/sensitivities/risks	**Discount rate (%)**
Key assumptions include the calculation of familiarisation and labelling costs to business. It has been assumed that manufacturers will not pass on one-off initial labelling and self assessment costs to consumers. Assumptions have also been made to estimate the benefit to consumers of adopting more secure IoT devices. This includes the extent of the adoption of more secure devices by UK consumers and the expected reduction in attacks as a result.	**3.5%**

Data from the Office for National Statistics Annual Survey of Hours and Earnings 2017 is used to provide an indication of familiarisation costs for businesses as a result of the legislation.

BUSINESS ASSESSMENT (Option A)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	**0.6**
0.1	**0**	**0.1**	

Summary: Analysis & Evidence Policy Option B

Description: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with manufacturers to self assess that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low:	High:	Best Estimate:
2017	2022	10	102.6	5131.1	2052.4

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost* (Present Value)
Low	0		Currently un-monetised	**0**
High	0		Currently un-monetised	**0**
Best Estimate	0		Currently un-monetised	**0**

*These costs are less than £10k, and have therefore rounded to 0.

Description and scale of key monetised costs by 'main affected groups'

Transition costs to UK manufacturers have been estimated, including the cost of familiarisation with legislation and the self assessment process. DCMS has estimated that there are approximately 69 consumer IoT manufacturers in the UK that will be affected. These are expected to be one off initial costs, so it is assumed that these costs will not be passed on to the consumer.

Other key non-monetised costs by 'main affected groups'

DCMS plans to use the consultation to collect data in order to estimate the cost to manufacturers of amending their production processes to comply with the Code of Practice guidelines. It is expected that these costs will be significant, and hence will significantly affect the outcome of the cost-benefit analysis. Enforcing minimum standards will likely have a disproportionate impact on small and micro businesses, which may create barriers to entry in the market. There will also be a cost to government of monitoring the sale of consumer IoT products on the UK market.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0		12.6	**102.6**
High	0		627.7	**5131.1**

Best Estimate	0		251.1	**2052.4**

Description and scale of key monetised benefits by 'main affected groups'

The main benefit of mandating that manufacturers and retailers comply with the top 3 Code of Practice guidelines is the reduction in attacks which exploit insecure IoT devices. This will lead to a reduction in the cost to consumers associated with these attacks.

Other key non-monetised benefits by 'main affected groups'

There is also a significant potential benefit to wider society of having fewer insecure IoT devices on the market open to hacking and use in wide-scale DDoS attacks, which can target infrastructure essential to the UK economy.

Key assumptions/sensitivities/risks	**Discount rate (%)**
Key assumptions include the calculation of familiarisation costs to business. It has been assumed that manufacturers will not pass on one-off self-assessment costs to consumers. Assumptions have also been made to estimate the benefit to consumers of adopting more secure IoT devices. This includes the extent of the adoption of more secure devices by UK consumers and the expected reduction in attacks as a result.	**3.5%**

Data from the Office for National Statistics Annual Survey of Hours and Earnings 2017 is used to provide an indication of familiarisation costs for businesses to understand how to properly implement the proposed legislation.

BUSINESS ASSESSMENT (Option B)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	**0**
0	**0**	**0**	

Summary: Analysis & Evidence Policy Option C

Description: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self assess and to ensure that the label is on the appropriate product packaging.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
			Low:	High:	Best Estimate:
2017	2022	10	202.4	7183.3	3077.4

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	0.3		Currently un-monetised	**0.3**
High	2.8		Currently un-monetised	**1.8**
Best Estimate	1.3		Currently un-monetised	**1.3**

Description and scale of key monetised costs by 'main affected groups'

The monetised costs to business include the cost of familiarising with legislation, self-assessing their product compliance and the cost of redesigning packaging to include the label. These are expected to be one off initial costs, so it is assumed that these costs will not be passed onto the consumer.

Other key non-monetised costs by 'main affected groups'

DCMS plans to use the public consultation to collect data in order to estimate the cost to manufacturers of amending their production processes to comply with all 13 of the Code of Practice guidelines. It is expected that these costs will be significant, and hence will significantly affect the outcome of the cost-benefit analysis. Enforcing minimum standards will likely have a disproportionate impact on small and micro businesses, which may create barriers to entry in the market. There will also be a cost to government of monitoring the sale of consumer IoT products on the UK market, and to retailers of checking that their products have the appropriate label.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0		25.1	**205.2**
High	0		878.8	**7183.5**
Best Estimate	0		376.6	**3078.7**

Description and scale of key monetised benefits by 'main affected groups' Consumers will benefit from their IoT devices complying with all 13 guidelines and thus being more secure (compared to their products complying with some, but not all, of the guidelines or not complying with any guidelines at all), resulting in fewer cyber-attacks.
Other key non-monetised benefits by 'main affected groups' Consumers will be able to identify the level of security and safety of their products through the label, whilst also being assured that their devices meet the minimum standards set out in the Code of Practice. The label will increase consumers' security awareness and may encourage consumers to take action to secure their existing products, leading to lower costs associated with breaches. There is also a significant potential benefit to wider society of having fewer insecure IoT devices on the market open to hacking and use in wide-scale DDoS attacks, which can target infrastructure essential to the UK economy.

Key assumptions/sensitivities/risks	**Discount rate (%)**
Key assumptions include the calculation of familiarisation and labelling costs to business. It has been assumed that manufacturers will not pass on one-off self-assessment costs to consumers. Assumptions have also been made about the extent of the reduction in attacks against consumer IoT devices, and the benefit that this will have to society in terms of reduced costs.	**3.5%**

Data from the Office for National Statistics Annual Survey of Hours and Earnings 2017 is used to provide an indication of familiarisation costs for businesses to understand how to properly implement the proposed legislation.

BUSINESS ASSESSMENT (Option C)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	**0.6**
0.1	**0**	**0.1**	

Contents

The scale of the Internet of Things

As the technological advancements of the 21st century continue to accelerate, consumers are able to purchase and bring more and more 'smart' devices into their homes, such as smart TVs, connected toys, smart music speakers and smart washing machines.

The Internet of Things (IoT) is already being put to effective use across a range of industries and it is delivering significant social and economic benefits[1] with the number of internet connected devices in use continuing to rise. Forecasts vary, but some suggest that there will be an estimated 20 billion internet connected devices worldwide by 2020.[2]

In the UK alone, it is estimated that in 2016 there were 13.3 million IoT connections. This is expected to rise to almost 60 million by 2020, and to over 150 million by 2024, of which around 40 million will be consumer electronics and fast-moving consumer goods.[3] Moreover, UK household ownership of smart devices could rise from approximately 10 devices per household today, to 15 by 2020.[4] The networks and data that flow from connected devices will also support an extraordinary range of applications and economic opportunities for society.[5]

The growth of IoT markets is also providing great opportunities for UK companies. In 2016, digital sectors contributed £116.5 billion to the UK economy - almost 7% of the UK's gross value added. Additionally, the export of digital sector services amounted to just over £32 billion in 2015.[6]

It is expected that by 2020 global annual revenues could exceed $470 billion for the IoT vendors selling the hardware, software and comprehensive solutions.[7] Experts predict that cloud service providers, analytics and infrastructure software vendors will have the most influence over IoT purchases.

---

[1] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[2] Gartner report on scale of connected devices by 2020, accessed at: https://www.gartner.com/newsroom/id/3598917, 2017. This figure excludes smartphones, tablets, and computers.

[3] Review of the latest developments in the Internet of Things, Cambridge Consultants for Ofcom, 2017. https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf

[4] WRAP report 'Smart Devices and Secure Data Eradication', 2016, accessed at: http://www.wrap.org.uk/sites/files/wrap/Data%20Eradication%20report%20Defra.pdf (forecasts taken from 17 smart product categories)

[5] Government Office for Science, IoT report, 2014, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[6] DCMS Sectors Economic Estimates 2017: Employment and Trade, 16 August 2017. Accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/640628/DCMS_Sectors_Economic_Estimates_2017_Employment_and_Trade.pdf

[7] Bain & Company, How Providers Can Succeed in the Internet of Things

What is Consumer IoT?

For the purposes of this Consultation Stage Impact Assessment, we have defined consumer IoT products as products that are connected to the internet and/or home network and associated services[8].

A non-exhaustive list of examples includes:

- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Smart cameras, TVs and speakers
- Wearable health trackers
- Connected home automation and alarm systems
- Connected appliances (e.g. washing machines, fridges)
- Smart home assistants

Problem under consideration

A 2018 survey of 3,750 consumers by Ofcom found that the most prevalent internet connected devices in the UK include:[9]

- Smartphones – used by 78% of respondents
- Smart TVs – in 42% of households surveyed
- Wearable devices – in 20% of households, including fitness trackers that monitor factors such as physical activity and location
- Smart speakers – in 13% of households, which can react to voice commands and be used to control other devices.

It is clear that consumer IoT products are prevalent in people's lives, but large numbers of these devices are sold to consumers without even basic cyber security provisions. Consumers are both unaware that their products are potentially insecure and are not provided with sufficient comparable information about the security of consumer IoT devices to allow them to make an informed purchasing decision.

Insecure consumer IoT can lead to people's privacy and safety being undermined because these insecure products are normally connected to people's home networks. If just one IoT device in a consumers network within their home has poor baseline security requirements, then this could allow a hacker/cyber criminal to easily infiltrate their entire network.

When security flaws of devices in the home are exploited, compromised services can cause significant problems. A device with a microphone or camera could be used to record individuals within their home, or information about their daily routine could be used without their knowledge, to exploit, harass or blackmail them. Some IoT products designed for

[8] https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security#scope-of-applicability

[9] Ofcom (2018). The Communications Market 2018.

children have had security issues that left voice recordings and imagery (that families believed were private) open to the public, or easily accessible for those wishing to exploit it.[10]

A compromised device connected to home heating or appliances may also cause safety risks - for example an attacker may be able to disable safety controls or deny usage, such as disrupting heating systems during winter. Alternatively if smart locks or connected physical access control systems are compromised, criminals could get into homes without needing to force entry.[11]

As the uptake of these products continues to grow, there is an emerging risk that large numbers of consumer IoT devices could be, and have already been used as part of a coordinated attack (known as Distributed Denial of Service Attacks, or "DDoS" attacks) in the future which could affect essential systems, such as electricity supplies.[12]

"DDoS" is short for Distributed Denial of Service. This is a type of Denial of Service attack where multiple compromised systems, which are often infected with a Trojan virus[13], are used to target a single system causing a Denial of Service attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Consumer IoT is a relatively new area of industry, meaning that the true costs of insecure devices and services on the market have traditionally been difficult to quantify. We are dependent on mainly qualitative assumptions, and research coming out of global institutions, to try and determine costs.

Researchers at the University of California sought to determine the cost of insecure IoT devices[14] by examining the impact of three different types of distributed denial of service attacks on IoT devices. Two real life attacks and one hypothetical attack were used as part of this research.

Based on energy and bandwidth consumption, the researchers estimated what costs would be incurred by consumers when their devices are used in these DDoS attack scenarios.[15]

---

[10] BBC News report, Connected Toys cyber breach, 2017, accessed at: http://www.bbc.co.uk/news/technology-39115001

[11] Engadget report on flaws in bluetooth locks, 2016, accessed at: https://www.engadget.com/2016/08/10/researcher-finds-huge-security-flaws-in-bluetooth-locks/

[12] Definition of DDOS attacks: Where a number of devices (which have previously been infected, for example by malware) communicate with each other at the same time to create a host which causes a network resource, (such as a web service) or targeted device to be significantly slower to respond or cease to function'

[13] https://www.kaspersky.co.uk/resource-center/threats/trojans

[14] https://groups.ischool.berkeley.edu/riot/

[15] Definition of device bandwidth: the amount of data that can be transmitted in a fixed amount of time

Table 1

Attack	Cost
Scenario 1: Krebs On Security Attack: A very large distributed denial-of-service attack (DDoS) against KrebsOnSecurity.com in 2016.[16]	According to their cost calculator, the total electricity and bandwidth consumption costs borne by consumers in this attack was $323,973.75.
Scenario 2: The Dyn, Inc. Attack	They calculate the total electricity and bandwidth consumption costs borne by consumers as $115,307.91.
Scenario 3: "Worst-Case" Attack. This hypothetical “Worst-Case” scenario approximates the costs that could result if the Mirai[17] botnet operated at its peak power.	The projected total electricity and bandwidth consumption costs to consumers of this attack is $68,146,558.13.

The University of California’s research was conducted during 2017 - 2018, with their study focused on malware taking over IoT devices because they had default credentials (which would be addressed if these devices did not have a default password, as advocated by guideline one of the UK Government’s Code of Practice for IoT Security).

Rationale for Government intervention

The UK Government wants to ensure that the UK is one of the most secure places in the world to live and do business online. To support these aims, the Government wants to make it as easy as possible for people to use internet-connected devices as safely as possible or without the burden of implementing security features within their personal devices.

The UK Government is world leading by being one of the first countries to mandate IoT security standards in consumer products. The UK is also leading efforts and collaborating with international governments and industry partners in IoT security to ensure that guidelines from the Code drive global alignment across the global IoT supply chain.

Currently there is a significant lack of information provided to consumers on IoT devices, particularly on the security features that are built-in to products.[18] DCMS commissioned a labelling survey of 6,482 consumers in January 2019 which included a question on the top

[16] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[17] https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
[18] PETRAS Report, ‘What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?’, December 2018. https://osf.io/preprints/socarxiv/63zkt/

four most important types of information for participants when buying smart devices. Three quarters (76%) noted cost, whilst nearly half (49%) of participants consider security features to be important in their decision-making process, with security features ranked significantly more important than other factors such as brand reputation, customer reviews, privacy features and design.[19]

However consumers cannot easily distinguish between devices with high and low quality security features, resulting in consumers putting themselves at risk of cyber-attack. The same DCMS survey found that of those that did not rank 'security features' in their top four criteria (3,317), 72% stated this was because there was an expectation that security was already built into the devices they were purchasing.

There is a lack of incentives for industry to provide security information to consumers, including a lack of coherent regulation, both within the UK and abroad, in this emerging space. Manufacturers will continue to make these insecure products and retailers will continue to sell them unless Government acts to address these problems.

Relying on industry to self regulate and voluntarily address the problem has not worked, with key disincentives for industry centred around cost of amending product lines across the supply chain. Moreover, companies who try investing resource into ensuring their products are secure can end up losing competitive advantage over their rivals.

It is also important to note that manufacturers do not face the immediate economic costs of a DDoS attack conducted through their devices, which is instead borne by consumers at overall projected total costs of up to $68 million[20] in the worst case DDoS attack scenarios, as previously mentioned.

The UK Government published the Secure by Design report[21] in March 2018, and subsequently published the finalised voluntary Code of Practice for Consumer IoT Security in October 2018.[22] The purpose of the Code of Practice is to improve the security of consumer IoT products and associated services which, if compromised, could potentially cause significant disruption to the UK economy, society and individuals' welfare. The Code encourages manufacturers to act responsibly by embedding good practice security requirements into their products.

However, with the Code being voluntary and there being no coherent legislation in place, there are only limited soft levers that Government can use to incentivise manufacturers and retailers to take action (e.g. voluntary pledging and voluntary labelling schemes).

---

[19] Consumer Internet of Things Security Labelling Survey Research Findings Report by Harris Interactive, February 2019.
[20] Scenario 3: "Worst-Case" Attack
[21] Secure by Design Report, Department for Digital, Culture, Media and Sport, 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
[22] Code of Practice for Consumer IoT Security, Department for Digital, Culture, Media and Sport, 2018 https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

The power of regulation is to force out the very worst practice we are seeing in the market (e.g. default passwords) and it is our best lever available to influence industry to meet these requirements. This is the key reason why the Government has publicly announced the intention to mandate appropriate aspects of the Code through new forthcoming legislative means.[23]

Policy objectives

The overarching policy objective of our work is to ensure all consumer IoT products are secure by design.

Option A of this impact assessment sets out how we will achieve this by informing consumers about the baseline security of the IoT products that they purchase. For the purposes of this impact assessment, we have defined the baseline security as the relevant aspects of the top three guidelines of the Code of Practice for Consumer IoT Security[24].

Through mandating that a label (positive or negative) must be placed on the product packaging and product websites, consumers will be aware of the baseline security features of consumer IoT devices and take this information into account to allow them to make more informed purchasing decisions.

We see this approach helping to achieve our overall objective in a proportionate way. The expected outcomes of this approach are changes in consumer behaviour, due to the label, incentivising manufacturers to make devices secure by design, resulting in better protection of people's privacy, online security and safety and consumer trust in manufacturers and retailers. If we proceed with this option we will also seek to review the impact of the label at a later date, with a view to pressing ahead with mandating the above mentioned security requirements outright if it is deemed that the label is not producing the desired effect of ensuring these IoT products are secure by design.

We also set out alternative routes to achieving this overarching objective through Options B and C within this Impact Assessment.

This work sits as part of a broader project that Government has undertaken since the Secure by Design review was first launched in January 2017. This work has been taken forward due to a specific objective in the Government's National Cyber Security Strategy (2016 - 2021), which outlines the Government's cyber security ambition over a five year period[25] and builds

[23] Informal Consultation Response to Secure by Design Report, Department for Digital, Culture, Media and Sport, 2018 https://www.gov.uk/government/publications/secure-by-design/government-response-to-the-secure-by-design-informal-consultation

[24] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[25] UK National Cyber Security Strategy, 2016, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

on the National Cyber Security Centre's (NCSC) existing technical guidance to industry published in May 2017.[26]

DCMS published the 'Secure by Design: Improving the cyber security of consumer internet of things' report in March 2018, which set out a number of proposals, including a draft Code of Practice for consumer IoT security. The report also signposted future work to develop a consumer IoT labelling scheme and create consumer guidance on smart devices in the home as part of the Government's efforts to work with industry and other stakeholders to address the challenges of insecure consumer IoT.[27]

There are many activities across Whitehall that also engage with this issue. The BEIS Consumer and Competition Policy team represent the UK Government in working groups for various European Commission directives, such as the Sales & Goods Directive and Digital Content Directive. The UK Government is aware that the directive references the seller's responsibilities when digital content is present. The BEIS Consumer and Competition team have begun work to evaluate the impact of this directive in the UK. Any decisions around this directive will be dependent on the UK Government's negotiations with the EU.

It should also be noted that IoT products primarily intended to be employed in manufacturing, transport, other industrial applications or healthcare are not in scope of the proposed regulation.

Smart Electric vehicle charge-points are not in scope of this work. The UK Government already has powers to ensure electric vehicle charge-points comply with requirements relating to security through the Automated and Electric Vehicles Act and is due to consult on these in Summer 2019.

What are the Code's top three guidelines trying to address?

Guideline 1: IoT device passwords must be unique and not resettable to any universal factory setting.

This problem has dated back years with manufacturers still not taking steps to address the issue of default passwords, as shown by the 2012 Carna Internet Census which found "several hundred thousand unprotected devices on the Internet".[28]

Passwords are an easily-implemented, low-cost security measure. Most consumer connected products will use a password, with the majority of these passwords being set to default during the manufacturing process. The most popular permutations of default

[26] National Cyber Security Centre website on secure by default, 2017, accessed at: https://www.ncsc.gov.uk/articles/secure-default
[27] Secure by Design Report, Department for Digital, Culture, Media and Sport, 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
[28] https://www.theregister.co.uk/2013/03/19/carna_botnet_ipv4_internet_map/

usernames and passwords tend to be “admin/admin”, “admin/0000”, “user/user”, “root/12345” and “support/support”.

Universal default passwords facilitate unauthorised access to devices. Such practice brings significant risk to consumers’ privacy and online security. Manufacturers and retailers are selling products with factory-set default passwords. This vulnerability is one of the most serious that can be found in IoT devices because the default passwords can be found online and easily used to target and gain access to internet connected devices.

This issue comes at a time when connected device ownership is growing. The Tech UK “State of the connected home” report[29] illustrates the increasing growth in the number of connected devices owned by consumers from 35% in 2017 to 44% in 2018. A 2017 Keeper Security survey[30] found that nearly three in four millennials in the 25-34 age range are not even aware that these devices arrive from most manufacturers with simple, pre-set default passwords. Some 65% of these millennials, who are the most active buyers of IoT devices, are not aware of the rising tide of concern around IoT device security.[31]

Most manufacturers do not offer consumers an easy way to change these passwords and they should not be burdened with responsibility, instead it should be placed on manufacturers to design devices with security built-in before they are placed on the market.

The Mirai botnet attack began[32] with IoT devices that had been infected by malware using a list of 62 standard passwords. After connecting to the network, each infected device started scanning for randomly generated IP addresses. What followed were huge DDoS attacks on the website of journalist Brian Krebs, Dyn Inc, a US internet service provider, Liberia, Deutsche Telekom and a US college. The botnet reportedly encompassed, from conservative estimates of 380,000 consumer IoT devices (reported to be up to 600,000 at its peak[33]) simultaneously.

It is clear that many of these products are being manufactured at a very low cost, and that basic security practices are not being followed.

Guideline 2: Manufacturers of IoT devices need to provide a public point of contact as part of a vulnerability disclosure policy

Vulnerabilities create opportunities for malicious attackers to commit cybercrime or disrupt user activity. Although some vendors may seek to identify and remediate vulnerabilities before their products and services are brought to market, testing for everything is impossible.

---

[29] https://www.techuk.org/insights/news/item/13914-connected-home-device-ownership-up-but-consumers-remain-sceptical

[30] https://keepersecurity.com/blog/2017/11/22/survey-says-iot-toys-high-holiday-wish-lists-security-not-much/

[31] https://keepersecurity.com/blog/2017/11/22/survey-says-iot-toys-high-holiday-wish-lists-security-not-much/

[32] https://www.theinquirer.net/inquirer/news/3008241/mirai-new-variant-of-botnet-turns-iot-devices-into-bitcoin-mining-slaves

[33] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

As a result, once products come to market, vulnerabilities may still be found in technology products and online services, either through intentional investigation or accidental discovery.

When vulnerabilities are identified, it is important that security researchers or discoverers have access to a clear and protected path to “disclose” their findings to technology developers, manufacturers, and service providers to help resolve issues without exposing users to undue risk. This mechanism should be part of an organisation’s vulnerability disclosure policy.

Alerts from security researchers can be an important early warning system for any organisation. Researchers should therefore be able to easily find a channel to report their findings, with manufacturers having a suitable internal facility in place to process these disclosures.

The Internet of Things Security Foundation’s report on vulnerability disclosure[34] found that 90% of the 331 global IoT companies researched had no form of vulnerability disclosure mechanism. This is a serious concern as it reflects a wider issue of poor practice.

In the absence of a vulnerability disclosure policy, companies can opt to create or use financial-based incentive schemes, commonly known as bug bounties. A bug bounty program is an initiative that sets out to incentivise security researchers (via financial rewards) to disclose vulnerability discoveries to the manufacturer or operator of the affected technology. The goal is to enable the technology provider or operator to address or mitigate the bug before the general public is aware of them and there is widespread abuse or exploitation of the vulnerability. Implementation of bug bounties is low across industry, and thus cannot be relied upon to mitigate the above mentioned risks.

Not only are there benefits to the consumer from companies having a vulnerability disclosure policy in place, but direct economic benefits were cited by just over half of the companies themselves in the National Telecommunications and Information Administration survey[35] as another motivation for utilising vulnerability handling policies. Specifically, 54% of companies reported that vulnerability disclosure and handling policies actually reduced the costs of marketing and development of their software products and services.

Although work has previously been undertaken to develop best practices for vulnerability disclosure and handling through voluntary International Standards Organization (ISO) standards[36], a significant amount of IoT manufacturers have not fully embraced the principles underlying coordinated vulnerability disclosure.

Without recognition of this situation and action by the manufacturers, security researchers may revert to disclosing security concerns publicly because they have no outlet to report vulnerabilities to these companies. This is problematic because it may create reputational

[34] https://www.iotsecurityfoundation.org/best-practice-guidelines/
[35]https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf
[36] ISO/IEC 291471 and ISO/IEC 301112 https://www.iso.org/home.html

damage for the companies concerned, leave a window of vulnerability for consumers using those products and impact confidence in the adoption of consumer IoT as a whole.

Guideline 3: Manufacturers of IoT devices need to explicitly state the minimum length of time for which the product will receive security updates

"End-of-life" is a term used to indicate that the product is at the end of its useful life (from the vendor's point of view), and a vendor stops marketing, selling, or undertaking work to sustain it (e.g. providing software updates).

Many of the devices involved in the Mirai attack either were out-of-date with their patching or simply could not be patched at all.[37] This means that the spread of Mirai could not easily be halted. Had software patching been available, devices could have been immunised and fixed. More importantly, regular patching also protects against future variants of attacks that exploit other vulnerabilities, neutralising their effect.

A published end-of-life policy provides transparency for the consumer especially on the support period for security updates. Manufacturers need to make clear the length of time that software updates will be provided after the sale of their device. For constrained devices with no possibility of a software update, the conditions for and period of replacement support should be clear. We have been working with colleagues across government to ensure that this is in line with the forthcoming Sale of Goods and Guarantees EU Directive.

Consumer IoT Security labelling scheme

At present, consumers are expected to conduct pre-purchase research and review products in store to find information on the security features of different IoT products before deciding on which device to purchase. This presents a wide array of issues because many consumers do not have the technical expertise to know what security features should be built into their devices. Moreover, a significant amount of manufacturers do not provide this information online or within product documentation.[38]

In the absence of a regulatory approach, a market failure will continue to occur whereby consumer decision-making is hindered due to information asymmetries because product security information is being withheld from consumers.[39] If consumers continue to struggle to assess product security (in terms of cognitive effort or time taken), then we risk creating a situation where they will negatively perceive IoT devices or connect devices to their home network which have serious vulnerabilities. These information asymmetries need to be addressed before they contribute to further market failures and cyber security attacks.

---

[37] https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[38] PETRAS Report, 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?', December 2018. https://osf.io/preprints/socarxiv/63zkt/

[39] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

Weaknesses in alternative options to a labelling scheme

DCMS advocates a labelling scheme, rather than stating that manufacturers should provide more material for consumer pre-purchase research because a positive and negative label would provide consumers with an easy solution to distinguish between products.

A further alternative approach to a labelling scheme would be to encourage consumer behaviour by conducting an awareness and behaviour change intervention. This campaign would be intended to motivate consumers to routinely assess the security of IoT devices that they are considering purchasing. However, if implemented alone, such an intervention would almost certainly fail for the following reasons:[40]

- Firstly, many manufacturers do not currently provide information about their devices' security features. Without this information, people would still be unable to assess the various levels of security in products.[41]
- Secondly, the average consumer will not (and the burden should not fall on them to) have the required expertise to assess this information if it were available.

Rationale for mandating a Labelling Scheme

There are a number of benefits from mandating a labelling scheme. These include that setting out the minimum baseline for security through a label could act as a lever to encourage companies to compete on security as a form of market differentiation.[42] It would also hold them to account, to some extent, by encouraging manufacturers to explicitly focus on the security of their devices and for this to be done against a clear criteria. In turn, this would allow market surveillance authorities and security researchers to be able to clearly assess a company's compliance to IoT security in a more consistent and accessible manner.

DCMS' preferred option is to mandate retailers to only sell consumer IoT products that have an IoT security label. We believe that this approach will incentivise manufacturers to make the necessary amendments to their supply chains and organisation so that they adhere to the top three guidelines in the Code or risk selling a product with a negative label. Consumers would then be able to make informed purchasing decisions based on the information provided to them. DCMS recognises that if the label is mandated then retailers will likely hold a significant amount of products in their warehouses that aren't labelled. DCMS will ensure that if following the consultation, a decision is taken to mandate the label, our timeline will allow for a voluntary labelling scheme launch before mandating it to give retailers sufficient time to ensure that they are not adversely affected by this proposal. This will also provide manufacturers with the time to make changes to their organisational processes and supply chain.

---

[40] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

[41] PETRAS Report, 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?', December 2018. https://osf.io/preprints/socarxiv/63zkt/

[42] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

Approach for creating the Labelling Scheme

DCMS's approach has focused on creating a label that was supported by an extensive evidence base and which was informed by feedback from an array of stakeholders. We have also engaged extensively with other international governments to promote this work and drive efforts to create global alignment on consumer IoT security. As part of this project, DCMS worked closely with the PETRAS Consumer Security Index Project to fund and compile a range of studies. This included PETRAS compiling a rapid evidence assessment on labelling schemes for IoT security which clearly set out the benefits of creating a labelling scheme for consumer IoT devices.[43]

DCMS also set up a working group which was made up of other government departments, such as NCSC and BEIS and external stakeholders, including industry and manufacturing associations, certification organisations, academics and consumer groups. The working group focused on reviewing DCMS's labelling options and creating an aligned approach on labelling for smart household devices. The working group agreed that a graded or tiered label, such as a food or 'energy rating' label would not be appropriate for consumer IoT devices. This was primarily because of concerns that consumers would struggle to differentiate between what the different levels and colours meant in terms of a products cyber security features. The working group supported the creation of a label which combined elements of an information label with a binary mark to ensure it conveyed useful information to consumers and was not too burdensome for manufacturers. The group agreed that the label's criteria should initially be based on the top three guidelines in the Code of Practice because many manufacturers would have to make modifications to their (likely international) supply chain. However, they agreed that the criteria should be reviewed at a later date to consider expanding it and DCMS should continue to push companies to implement all thirteen of the Code's/ETSI TS's steps.[44]

To help anaylse various labelling options, DCMS part-funded a survey study, conducted by researchers at the Dawes Centre for Future Crime at UCL between September 2018 to January 2019, to assess the influence of different (security-related) labelling schemes on consumer choice for IoT devices. Using a stated preference discrete choice approach, 3,000 participants were asked to make decisions about which devices they would purchase, with the devices varying in terms of functionality, price and whether they carried a label or not. Questions were asked about four different types of consumer IoT devices, and the effects of different labels on participants choices tested. The survey results indicated that:

[43] PETRAS IoT Hub, Rapid evidence assessment on labelling schemes and implications for consumer IoT security, October 2018. https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security

[44] We welcome industry to create certification frameworks that are based on the Code and ETSI TS. We are aware that the British Standards Institute has created an Assurance Framework based on all thirteen guidelines in the Code.

- For nearly all labelling scheme options, participants favoured a device that had a label over one that did not.[45] The exception was for a graded label that indicated that the device had a poor level of security.
- Relative to the average price of devices on three major UK retailers websites (used in this study), the findings suggested that for the four labels that had the most positive effects on decision making, on average participants were willing to pay an extra 34%, 19%, 27%, and 22% for additional security for Smart Security Cameras, Smart TVs, Wearables (such as a FitBit), and Smart Thermostats.
- When asked to rate how much they would use the various labels to help them buy and compare products, for both questions, participants responded that they (moderately to strongly) agreed that they would.[46]

To support DCMS with creating the labelling designs, DCMS funded Make it Clear, a design company, to review 40 different consumer IoT products in stores to evaluate the scope, placement, prominence and presentation of labels on their packaging. Make it Clear's research highlighted that the UK Government's labelling scheme would need to compile detailed usage guidelines for manufacturers to ensure that consumers can clearly see the labelling scheme on product packaging. Moreover, the findings recommended that the UK Government's labelling scheme should be predominantly black and white in colour because it would not add extra colours to a packaging printing process which would therefore limit the cost impact on manufacturers. Additionally, it would reduce the risk of the label clashing with any existing manufacturer product branding or conflicting with bold colours on the packaging.

Using this evidence, feedback from the working group and engagements with NCSC, four labelling designs were compiled and DCMS funded Harris Interactive to conduct a study involving 6,482 UK consumers to work out which was the most effective design.[47] The study was based on an approach whereby participants were split into 16 cells (roughly 400 people in each cell) and reviewed one label design and one smart product to also help address any unconscious bias.[48] The key findings from the study were:

- 93% of participants preferred a device with a label over a device without a label.
- 73% of participants stated it was important or very important to introduce a labelling scheme based on DCMS labelling designs. This contrasts with only 11% stating it was not important.
- At the overall aggregate level, based on DCMS's labelling designs, 6 in 10 people would purchase a labelled product at a 5% price premium.

[45] Please note that a participants age, gender or self-reported security behaviour did not seem to affect the participants labelling preference or willingness to pay.
[46] Johnson, S.D., Blythe, J.M., Manning, M., and Wong, G. (2019). The impact of IoT security labelling on consumer product choice and willingness to pay. https://osf.io/preprints/socarxiv/4yxp2/
[47] Quotas were used to ensure participants were representative of UK demographics in terms of age and gender. Results were weighted on age and gender to meet census data for UK citizens aged 16+ to ensure the sample was as nationally representative as possible, however only minimal weighting was required.
[48] Four smart products were tested from different categories that are part of consumer IoT. These were a smart TV, smart thermostat, internet-connected toy and a wearable device.

- The Icons with Text Underneath design ranked highest out of the four labels across every monadically-tested metric, such as ease of understanding and influencing consumers to switch brands if a product had the label.

DCMS considered whether a digital label, such as a QR code would be more appropriate for an IoT security label. In this instance, manufacturers would put a QR code on each product and be required to update their product websites so that consumers could access the latest security information on their devices. However, this option was disregarded for several reasons including that:

- A QR code would put a significant financial and time burden on manufacturers because not only would they need to design a QR code for each product, but they would also be required to keep information linked to the QR code up to date.
- Consumers would be burdened with having to regularly check the QR code for the latest information. Additionally, consumers are likely to recycle or dispose of their packaging based on the Government's latest advice rather than keep the QR code label for each of their various devices.
- Furthermore, the Harris Interactive survey highlighted that 46% (2,957 people) did not know how to scan a QR code on their phone to access information. Also when asked how many times in the last year participants had scanned a QR code to access information on a device or other physical product, the average answer was 1.8 scans per year with 57% stating they had never scanned.

DCMS also funded Make it Clear to review the same 40 different consumer IoT products on four different retailers' websites (John Lewis, Amazon, Google Shopping and Currys) and the manufacturer's product website. The study examined how, where and in what format labels are currently presented online. The findings highlighted that:

- Only 24% of the pages reviewed displayed a labelling scheme using an image or symbol (18% of retailer websites and 43% of manufacturer's product websites).[49]
- 36% of the pages reviewed referenced labelling within text on the product websites, however multiple clicks were needed to identify this information, usually within the product description or specifications table.
- None of the products reviewed contained hyperlinks to an external label website.

Based on the findings of Make it Clear's online study, if DCMS decides to mandate the label following the consultation, then it will consider mandating usage guidelines for the label to ensure that it is effectively highlighted on product packaging and also online, such as retailers websites and manufacturers product websites.

The draft designs for the labelling scheme that we are consulting on can be found in the Consultation paper. We are conscious of trademark requirements surrounding the use of

[49] Where label icons/images were shown on retailer websites, the majority were found on product images often in a section including multiple images with the ability to scroll through them. On manufacturer websites the majority of visual labels were found towards the end of the product page with compatibility/connectivity (30%), awards (11%), and energy/efficiency (8%) being the most common label types.

generic icons and are currently seeking legal advice on this. We considered creating unique shapes for each icon, however we assessed that this would create strong challenges in explaining the meaning of the label to UK consumers.

Additionally, the Harris Interactive survey included a question which asked if the icons were suitable for the proposed criteria. 92% stated that the shield and arrows were the best designs for the label. The highest alternative option (a padlock) was suggested by less than 1% of the survey sample.

We welcome feedback on the designs and will consider making modifications to the label design following the consultation before launching it as a voluntary scheme later this year.

Rationale for proposed approach to regulation

The Government undertook a mapping exercise of the existing regulatory landscape to ascertain whether the Code of Practice for Consumer IoT Security is legally enforceable through existing data protection or consumer legislation (see appendix C). Whilst there are aspects of guidelines which do align with key principles of the Data protection Act 2018 and the Consumer Rights Act 2015, alignment does not equate to enforceability (with the exception being guideline eight which is enforceable through the Data Protection Act 2018).

The Code's top three guidelines

The assumption is that due to the vast amount of products that fall within the scope of what is considered "consumer IoT", any legislative intervention is likely to have a varying degree of impact on a large number of businesses and their supply chains.

A large proportion of companies within the complicated IoT supply chain are not located within the UK, so there will be substantial costs to the supply chain to ensure that the products become compliant.

We held a number of confidential workshops with NCSC, IoT security experts, a standards body, manufacturers, retailer associations and a Tech association to help us define how many guidelines of the code should we focus on regulating to start with, and how.

By weighing up the impact on businesses against the priority of ensuring that consumers are not burdened with implementing security measures, we have developed the below regulatory options based on the code's top three guidelines and how they would interplay with a consumer IoT security label.

In the absence of mandating all 13 guidelines, we are advocating that the top three (i.e. no default passwords, vulnerability disclosure, end of life policy) should be the minimum security requirements for manufacturing consumer IoT products and thus act as a minimum baseline in which to measure how secure the product is. This was agreed at the workshops.

Mandating the three guidelines would bring a quicker impact within a short amount of time and, from an enforcement perspective, is easier to test - products either meet these requirements or they do not.

Maturity approach

Feedback from the above mentioned workshops indicated that going straight to mandating the top three guidelines of the code would likely result in a number of unintended consequences, including an increased risk of “fire sales” of products prior to the legislation coming into force, potentially resulting in even more insecure IoT flooding onto the market. A notable potential issue raised was also the cost of immediate compliance with the top three guidelines and how this would affect existing supplier contracts.

Therefore, our preferred approach is to mandate retailers to only sell consumer IoT products that have a positive or negative IoT security label, with manufacturers to self assess and implement a security label on their consumer IoT product packaging. The criteria of the label is aligned with aspects of the security requirements set out in the top three guidelines.Manufacturers and retailers will also be mandated to signpost the label clearly on consumer IoT product websites.

Regardless of which option we progress with, we will look to introduce the label on a voluntary basis this year. This will ensure that the financial disruption to businesses is kept to a minimum (detailed rationale for this approach is set out later on in the “policy options” section) as a voluntary take up of the requirements will give industry the necessary grace period to implement the top three security requirements whilst at the same time increasing consumer choice that will influence the market to move away from producing and selling products that do not adhere to the top three guidelines.

Once this approach has matured, we will review how industry has responded to the label and whether this has resulted in the desired secondary effect of all consumer IoT products sold on the UK market to be secure by design. If industry have not taken sufficient action, we will seek to mandate the three security requirements outright.

As part of a phased approach to regulation, we will also examine at a later date whether to expand the criteria of the label to include additional guidelines of the Code of Practice. As previously stated, our long term ambition is for manufacturers to be compliant with all of the code to ensure that consumer IoT products available on the UK market have strong cyber security built in by design.

Regulatory Structure

We intend to create Primary legislation that gives the UK Government the ability to set the requirements for a mandated labelling scheme and/or to set security requirements for devices on sale in the UK.

Once this has been established, we will create Secondary legislation that sets out these requirements, with further secondary powers to mandate further guidelines of the Code of Practice at the appropriate time.

Policy Options

We intend to consult directly with retailers and manufacturers on these options during the consultation period.

Option 0: Do nothing

Under this option, the Government will take no more action than is currently planned to encourage the uptake of the security label:

- The Code of Practice would remain voluntary.
- The Government would continue to encourage companies to publicly pledge to voluntarily implement the Code within their production process. It should be noted that the Secure by Design report was published in March 2018 and at this time only a handful of companies have signed up to pledge.
- The Government would continue to encourage global adoption of the newly created industry standard, ETSI Technical Specification 103 645, which is based on the Code of Practice.[50].
- The Government would roll out the voluntary consumer IoT labelling scheme but we do not anticipate that there would be a high uptake of the scheme due to the cost to business of adopting the label and the continued lack of incentives for producers to provide this information to consumers.

Option A (preferred option): Mandate retailers to only sell consumer IoT products that have the IoT security label, with manufacturers to self declare and implement a security label on their consumer IoT products.

The Government is developing a product security labelling scheme which will first be voluntary and then mandated once the relevant bill has achieved royal assent. The voluntary labelling scheme will contain the same requirement as set out in this proposed option.

The label must indicate whether the product adheres to the following three aspects of the Code of Practice, namely that:

- All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.
- The manufacturer shall provide a public point of contact as part of a vulnerability

50 https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security

disclosure policy in order that security researchers and others are able to report issues.
- Manufacturers will explicitly state the minimum length of time for which the product will receive security updates

Consumers would be able to make an informed purchasing decision based on the information presented to them by the label. Purchasing products that adhere to the Code's top three requirements will better protect their privacy, online security and safety, and help mitigate the risk of DDoS attacks which exploit vulnerabilities in insecure consumer IoT devices.

We would be mandating retailers to sell consumer IoT products that have a security label on them which evidences that the product does or does not comply with the above-mentioned aspects of the Code.

Manufacturers would be expected to self-declare whether their products comply with the Code and communicate this via the label. This ensures that what is stated on the label is not misleading.

Rationale for mandating Labelling Scheme rather than the Code of Practice guidelines

DCMS' preference to mandate implementation of a labelling scheme instead of mandating product manufacturers to implement the top three guidelines is due a number of reasons, including:

- Advice received by the NCSC indicates that several manufacturers would struggle implementing these guidelines, and so a more flexible approach is needed which a labelling scheme delivers.
- A labelling scheme will mean that in future the UK could modify the criteria to increase the number of guidelines that signify the positive security label.
- An increasing number of countries are currently considering creating a labelling scheme for consumer IoT products. Seen as the world leader in IoT security, the UK has built up an extensive evidence base and creating a successful IoT security label would help promote cyber security best practice worldwide by encouraging other countries to follow in our footsteps.

As part of the consultation process, we will be seeking views from stakeholders as to how best to approach issues associated with existing consumer IoT devices on the market that will not have a label and how the proposed regulatory approach will impact on retailers who will have existing consumer IoT stock. We will also look to consult on how best to enforce these requirements, including which new or existing agency is best placed to undertake enforcement and whether additional penalties would need to be set out to ensure that companies correctly use the labels.

Option B: Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines, with the burden on manufacturers to self declare that their consumer IoT products adhere to the top three guidelines of the Code of Practice for IoT Security and the ETSI TS 103 645

Retailers would not be allowed to sell consumer IoT products that do not adhere to the following security requirements:

- All IoT device passwords shall be unique and shall not be resettable to any universal factory default value.
- The manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.
- Manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

Manufacturers would self declare whether their product adheres to the above three security requirements and communicate this to the retailer, (such as within a contract). The manufacturer would ensure that they are providing the retailer with products that are compliant.

We envisage that this option will encounter a large amount of pushback from manufacturers, because through the absence of current specific legal requirements, the assumption is that a high proportion of relevant devices on the market do not presently meet these requirements. We have commissioned external suppliers to undertake research to ascertain evidence as to how many relevant devices currently on the market do not meet the above mentioned security requirements. We anticipate that this piece of evidence work will be completed by Spring 2019.

As part of the consultation process, we will be seeking views as to how best approach issues associated with existing consumer IoT devices on the market that will not have a label and how the proposed regulatory approach will impact on retailers who will have existing consumer IoT products in their stock. We will also look to consult on how best to enforce these requirements, including what agency is best placed to undertake enforcement.

Option C: Mandate that retailers only sell consumer IoT products with a label that evidences compliance with all 13 guidelines of the Code of Practice, with manufacturers expected to self declare and to ensure that the label is on the appropriate packaging.

The assumption is that due to the vast amount of products that fall within the scope of what is considered “consumer IoT”, any legislative intervention is likely to have varying degrees of impact on a large number of businesses and supply chains.

Compliance will all 13 of the IoT Code of Practice guidelines will create a further barrier to entry for UK IoT firms. This could stifle innovation in the UK technology sector, due to the high level of regulation in comparison to the rest of the world, resulting in lower levels of investment into the growing IoT market.

A large proportion of companies within the complicated IoT supply chain are not located within the UK, so there will be substantial costs to the supply chain to ensure that the products become compliant. This may result in a reduction in competition, giving large firms who are more able to meet the minimum standard a competitive advantage. Therefore, it is not practical or cost effective to mandate that all manufacturers must adhere to all 13 standards set out in the Code of Practice at this time.

Option D: Adopt a potential consumer IoT certification scheme that may emerge from the EU cyber security certification framework being established by the EU Cybersecurity Act

In December 2018, political agreement was reached on EU Regulation 2017/0225 ('the Cyber Security Act'). This Regulation, when enacted, will strengthen the mandate of the European Union Agency for Network and Information Security (ENISA) and establish an EU cyber security certification framework, under which cyber security certification schemes across the EU will be harmonised.

While the Regulation is unlikely to be enacted before the UK exits the EU, assuming that a Withdrawal deal has been agreed, the UK will be legally obliged to implement the Regulations during the Implementation Period. While parts of the Regulation that apply to the establishment of national cybersecurity certification authorities and their functions do not come into effect until 24 months after the date in which the Act is published in the European Journal, the development of schemes will continue in haste and it is likely that schemes may be implemented during the Implementation Period.

The development and introduction of a consumer IoT certification scheme is likely to be high on the agenda. While we don't yet know the details of any such scheme, the Regulation states that schemes shall include reference to international standards followed in the evaluation (Article 47; Clause 1(b)). One relevant standard is ETSI Technical Specification 103 645.

The UK could therefore try to influence and adopt a potential consumer IoT certification scheme that may emerge from the EU cyber security certification framework being established by the EU Cybersecurity Act. Following the Implementation Period we could seek a mutual recognition agreement to continue to provide certificates under the scheme.

Cost Benefit Analysis

The following Section summarises the analytical approach to assessing these options and results, while further detail on the assumptions and modelling approach are set out in Annex D. However, we will seek to gather further evidence as part of the consultation to inform the evidence base prior to the final stage Impact Assessment.

This section of the impact assessment assesses the likely costs and benefits that will accrue to different groups affected by the proposed regulation.

Limitations of the calculations and estimates

This consultation stage impact assessment makes an initial estimation of costs and benefits of the option routes under consideration.

While this impact assessment brings together evidence from a number of sources, we would like to note there are still a number of limitations to the analysis that we are looking to address in this consultation.

Due to the lack of available evidence on the current IoT market, measuring economic impact can be challenging. There are no widely-accepted metrics for the state of IoT development, activity and adoption: insights come from unconventional datasets.[51] Future predictions are often funded by the tech sector, large management consultancies or technology analysts. Although the research base is growing, research methodologies are not always robust.

Throughout this impact assessment, it has been assumed that all fixed costs are absorbed by businesses (retailers and manufacturers) and marginal costs are passed onto consumers. Fixed costs include one off familiarisation, and label redesign costs. Marginal costs include amending the production process in order to meet the Code of Practice security standards. This simplifying assumption has been made as the fixed costs identified are deemed to be relatively small, so are unlikely to affect prices faced by UK consumers. Moreover, fixed costs are not affected by the volume of output produced, so the cost can be spread across output. However, this may not be the case in reality and DCMS is seeking advice on these assumptions in the consultation.

The figures presented in this impact assessment are based on the best available data and our best efforts to align this with the definitions used in the Code of Practice and labelling scheme. As such a large proportion of the population own IoT devices, estimates are very sensitive to changes in these assumptions, which we have tried to account for using sensitivity analysis.

We have commissioned external contractors to undertake a thorough evaluation of our proposed intervention and expect the finalised results of this work in March 2019.

[51] SQW (2016) *Evaluation Scoping Study and baseline for the IoT UK Programme*, Annex B

Therefore, the figures presented in this impact assessment should only be seen as indicative, and not considered to be the final estimates for potential costs and benefits under this proposed legislative intervention.

Counterfactual

Policy options A, B, C and D are assessed against the “Do Nothing” option (“the counterfactual”).

It is assumed in the “Do Nothing” option that the labelling scheme will remain voluntary. From our stakeholder engagements, we do not anticipate a high rate of adoption of the label in the absence of legislation due to the cost of adopting the label, and the lack of incentives for businesses to declare security measures of their products.

In this case, only organisations with already secure products would adopt the label if they believe that the cost of producing the label will be outweighed by the benefits of increased sales, leading to higher net profits. However, from our engagement with industry, we know that the majority of products do not comply with the top 3 Code of Practice guidelines. A voluntary label will not create strong enough incentives for manufacturers to produce secure by design products.

If the policy is successful, the main benefits will accrue through:

- Increased awareness of the security features in consumer IoT devices, leading to more informed purchasing decisions;
- Incentivising manufacturers to produce more secure products that comply with the top 3 guidelines in the Code of Practice;
- A reduction in the number of insecure IoT devices in UK homes;
- A reduction in the cost of cyber attacks caused by insecure consumer IoT devices;

The main costs of the regulation will be:

- Cost to businesses of familiarisation, labelling and self-certification
- Cost to business of voluntary/mandatory security improvements
- Cost to government or other authority of enforcing this regulation

Table 2 summarises the expected costs and benefits of the proposed regulations:

Type	**Costs**	**Benefits**
Direct	Familiarisation costs	Reputational benefits
	Self-certification costs	Reduced incidence of cyber attack
	Labelling costs	
	Retailer inspection costs	
	Disposing of legacy stock	
	Monitoring costs	

Indirect	Cost of security improvements	Wellbeing benefits

Cost of Cyber Crime

The cost of cyber crime is difficult to quantify, due to the lack of available data on the cost of cyber-attacks on individuals through their personal IoT devices. Moreover, not all cyber attacks result in a cost at all. There are a vast range of costs that are not only financial, but also non-monetary. This could include, for example, the time that it takes to re-secure networks after an attack, loss of personal data, effects on mental health and well-being, as well as the loss of internet access and the use of their internet connected devices.

The Home Office published The economic and social costs of crime[52] report in 2018. Their estimate of the average cost of cyber crime to individuals was £260 per incident (2015/16 prices, £271.21 in 2017/18 prices),[53] which took into account damage/lost property, physical and emotional harm, lost output and health services.

This is greater than the £121 loss per victim[54] estimated by Symantec for Norton security company in 2018. However, this would be expected as this figure doesn't take into account social costs occurring as a result of an attack.

There is a wide range in the value of estimates of cyber crime to the UK, with Detica estimating a cost of £27 billion to the UK economy, and a cost to UK citizens of £3.1 billion,[55] while Symantec estimates a total financial cost to the UK of £4.6 billion.[56] The 2018 Cyber Security Breaches Survey found that the average cost of cyber breaches for businesses was £1,230 per year.[57]

Statistics from the Crime Survey for England and Wales[58] have been used to estimate the number of cyber crimes that occur on an annual basis. It should be noted that the scope of the survey does not encompass Scotland and Northern Ireland, however the regulation will apply to the entire UK. Moreover, not all of these crimes committed against individuals would have been enabled by an IoT device.

There is a lack of data on the level of cyber crime in Scotland, which we will look to investigate further during the consultation. For example, only 47 cases of computer misuse were recorded as being reported to the Scottish police in 2016/17, highlighting the problem

[52] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf
[53] Taking into account inflation using HMG GDP Deflator Series (Dec 2018).
[54] http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2017-NCSIR-global-results-UK.pdf
[55] The cost of cyber crime, Detica in partnership with Cabinet Office, 2011.
[56] http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2017-NCSIR-global-results-UK.pdf
[57] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
[58] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

of underreporting. It is expected that further data from the Scottish Crime and Justice Survey will be available in late 2019/early 2020.[59]

Therefore, the figures presented below may not provide an accurate estimate of the cost of cyber crime in the UK.

Table 3: Number of cyber crime incidents

Sept 2016	Sept 2017	Sept 2018
3,824,030	3,271,750	2,878,600

Source: Crime Survey England and Wales

The incident figures in table 3 were calculated by taking the proportion of total computer misuse and fraud cases which were categorised as a cyber crime (93% and 56% respectively), and adding these figures to get a cumulative cyber crime figure for the given year.

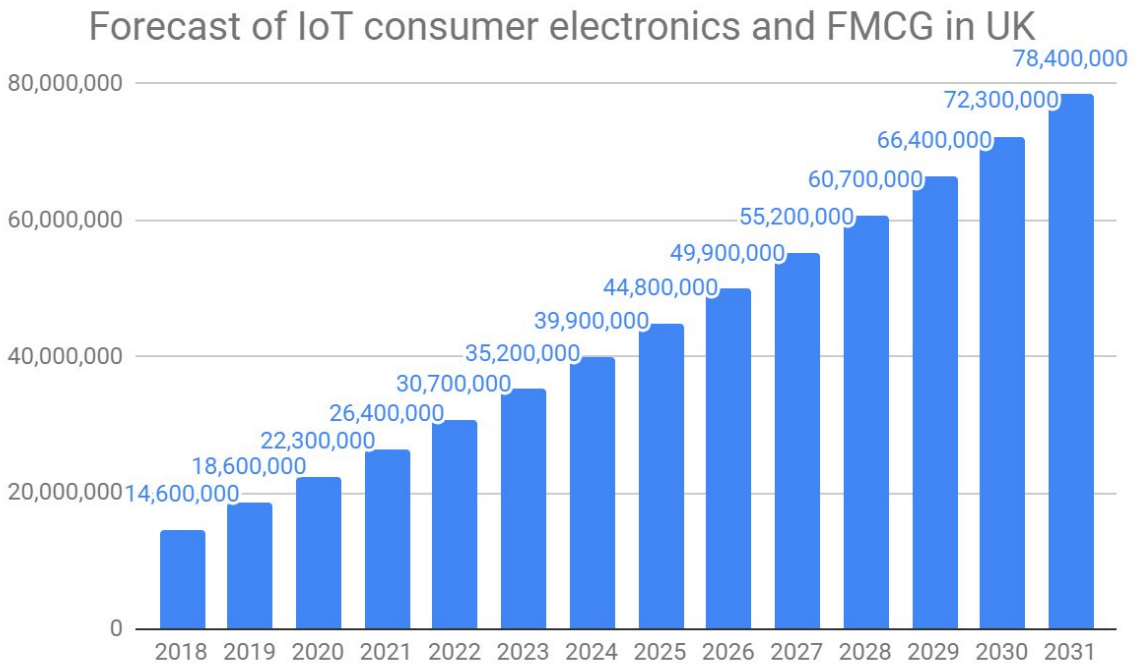
Assuming that the level of cyber crime is uniform across the UK, population statistics from the ONS can be used to scale up the figures to calculate the number of incidents for the entire UK population.[60] The population of England and Wales represented 88.9% of the UK population in 2017. Assuming that this proportion remains constant, this suggests that the number of cyber incidents in the entire UK in 2017/18 was 3,238,020.

Taking this as a proportion of the UK's total population, assuming one incident per person, 4.9% of people were victims of cyber attack in 2017/18. We have assumed, therefore, that 5% of IoT devices will be impacted by cyber attacks.

It is expected that the threat of cyber crime will continue to increase with the number of IoT products. Cambridge Consultants, as research on behalf of Ofcom, forecast the growth in consumer electronics and fast moving consumer (FMCG) IoT goods in the UK between 2018 and 2024.[61] DCMS has extended this forecast to 2031, by assuming that the increase of 200,000 products per year from 2021 will continue to 2031.

Figure 1

[59] Cyber crime in Scotland: evidence review, Scottish Government, 2018.
[60] Population estimates for the UK, England and Wales, Scotland and Northern Ireland: mid-2017, Office for National Statistics.
[61] Review of the latest developments in the Internet of Things, Ofcom, 2017.



Source: Review of the latest developments in the Internet of Things, Ofcom, 2017 (trend extended to 2031 by DCMS).

Therefore, assuming that 5% of IoT devices are impacted by cyber attack, and that this remains constant over time, figure 1 provides a forecast of the number of IoT cyber attacks in the UK annually. In 2018, this was estimated to be 730,000. The annual total cost of cyber attacks to UK IoT consumers can hence be calculated by multiplying the average cost (£271.21 in 2017/18 prices) by the estimated number of products affected (730,000 in 2018), to give a total cost of £197,986,752 in 2018.[62]

Research suggests, however, that the number of attacks is growing, with an increase in overall IoT attacks in 2017 of 600%.[63] This indicates that the threat is growing, along with the number of IoT devices, resulting in increasing risks and costs for consumers.

As part of the consultation, DCMS welcomes any further evidence on the cost of cyber breaches to IoT consumers in the UK, and the incidence of attacks against IoT devices.

Number of IoT Manufacturers

The IoT sector is relatively young and rapidly growing, meaning that it is difficult to estimate the number of IoT manufacturers, specifically producing consumer IoT products. This has proven a challenge for the forthcoming analysis, as the vast majority of consumer IoT products purchased by UK consumers are manufactured abroad. IoTONE has estimated that the number of suppliers in the consumer and household IoT goods sectors is 311.

[62] Sensitivity analysis assuming that 1% and 10% of IoT devices were targeted in 2018 gives annual costs of £39,597,350 and £395,973,504 respectively.
[63] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Including electronics and embedded devices increases this to 874 suppliers. However, only 37 of these have their HQ in the UK, and not all of these firms may supply UK consumers.[64]

The number of UK manufacturers of consumer IoT goods has been estimated using data from IoT Nation's online database.[65] The database was compiled using sectoral descriptors, and identifying companies that included reference to IoT on their website. As a result, these figures may not capture the entire IoT manufacturing sector in the UK.

Filtering for companies that are classified as manufacturers of computers, electronics and light electricals identified 69 companies based in the UK. Of these 69 companies, 21 were classified as micro, 27 SMEs, 8 mid-sized, 1 large and 12 unknown sizes.[66]

As part of the consultation, DCMS is requesting data and research on the number of IoT manufacturers and retailers which sell their goods on the UK market.

Familiarisation Costs

Costs will be incurred by businesses as they familiarise themselves with the legislation and its implications for their firm.

The wages for the legal profession and information technology and telecommunications directors are taken from the ONS' ASHE 2017.[67] The median is used as a best estimate, as it is believed to be the most representative wage (it's less skewed by outliers).

Table 4: Wage per hour: Annual Survey of Hours and Earnings (2017)

	Hourly wage rate		
Job Title	Best estimate (median)	Low (20th percentile)	High (80th percentile)
Legal professional n.e.c	£40.87	£25.00	£54.63
Corporate manager	£23.35	£13.77	£39.23

The 20th and 80th percentiles were chosen as high and low estimates, as these were the highest and lowest percentiles that were available for all categories analysed. Overhead charges of 30% are added to the wages, in accordance with the International Standard Cost Model Manual.

To estimate the total familiarisation cost, the number of hours to familiarise with the legislation is multiplied by the average hourly wage rate (upscaled by 30% to reflect

[64] https://www.iotone.com/suppliers
[65] https://iotuk.org.uk/projects/iotuk-nation-database%E2%80%8B/
[66] Ibid.
[67] https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

overhead charges) for each profession. This is then multiplied by the total number of businesses affected.

As familiarisation costs are a one off initial cost, it is assumed that foreign manufacturers would not pass this relatively small cost onto UK consumers. Therefore, the cost to business of familiarisation is only taken into account for UK based manufacturers.

The number of hours taken to familiarise with the legislation will vary between policy options due to differences in the requirements placed on businesses. Furthermore, there is a lack of evidence on how these costs will vary by business size. For micro and small businesses, which have fewer resources to manage the change in the regulation, the burden is expected to be greater.

It is also expected that businesses may employ lawyers to help businesses to familiarise with the mandated guidelines. From DCMS' initial industry engagement, micro and small firms are not expected to employ lawyers to familiarise with the legislation, however for the purposes of this analysis, we will assume that they do.

The following analysis will only take into account the impact of familiarisation on the 69 UK businesses identified as manufacturers of IoT. This is because the cost of familiarisation is relatively small, so it is unlikely that foreign manufacturers will pass on the cost to UK consumers through increased prices.

Moreover, the following analysis has not taken into account the cost of familiarisation for UK retailers, due to the high level of uncertainty around the number of retailers of consumer IoT devices in the UK, and what familiarisation with the legislation will involve for sellers. We plan to explore this further in the consultation.

As part of the consultation, DCMS plans to consult further with legal professionals, as well as wider industry, to request estimates for the number of hours it would take businesses of different sizes to familiarise with this legislation.

Self-Assessment Costs

Manufacturers will incur self-assessment costs to varying degrees under all three policy options. This will involve time spent gathering evidence as to whether a product does or does not comply with the regulation. This may involve gathering information from businesses which provide component parts as part of the supply chain.

The median hourly wage of a planning, process and production technician (£15.67) is used to calculate the best estimate of time cost to businesses. Sensitivity analysis is further conducted using hourly wage of the 20th and 80th percentile (£12.28 and £19.02) from the ONS' ASHE 2017.[68]

[68] Annual Survey of Hours and Earnings (ASHE), ONS, 2017. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

It has been assumed that the average number of consumer IoT products per manufacturer in the UK is 6 (upper and lower estimates of 10 and 2 respectively).[69] This is because IoT manufacture is a new and growing sector in the UK, which is mainly comprised of small and micro businesses, who are likely to have fewer products than multinational enterprises. Any further evidence on this assumption would be welcomed.

We envisage that any proposed regulator will not require to be informed of the self-certification information, which will mean that the administrative burden on manufacturers is lower. However, they will need to provide evidence of their rating if requested.

Self-assessment costs will only be incurred initially, and as producers redevelop existing and new products. In this market, new products and models are continually developed, however, the cost of identifying security features (default passwords) is part of the normal development process, so it is assumed that foreign manufacturers will not pass on this relatively small cost to UK consumers. Therefore, the cost to UK based manufacturers is only taken into account for this analysis.

DCMS plans to consult on potential methods of self-assessment and the relative costs to business these will incur. Any further evidence on the average number of IoT products produced in the UK per business would be welcomed.

Labelling Costs

The following analysis is only relevant for policy options A and C, where a security label is mandated.

The cost of producing the label will depend upon the type of label that is used. DCMS are currently consulting on which labelling option would be most effective. The design of the label will be black and white in order to minimise costs for manufacturers.

There are several options for labelling, which makes estimating these costs difficult. This includes stick on labels versus redesigning and printing the symbols directly onto current product packaging.

As foreign producers will likely sell to other markets where the label is not mandatory, they may choose to opt for a stick on label for products which are being exported to the UK. This would incur a cost of designing the label, rather than the packaging, and a small marginal cost per product. Therefore, there is a risk that this small marginal cost may be passed on to UK consumers, although this would not be significant in proportion to the price of the good.

However, research on the cost of labelling changes for food manufacturers[70] states that it is unlikely that manufacturers would opt for a stick on label for the following reasons:

[69] Assumption made from simple online search.
[70] Developing a Framework for Assessing the Costs of Labelling Changes in the UK, Campden BRI for DEFRA, 2010.

- Stickers do not look as professional as pre-printed packaging,
- Adding adhesive labels after packaging is inefficient, lowers productivity and may require extra equipment,
- Consumers perceive products with additional labels as suspicious and lower quality.

Therefore, it has been assumed for the purposes of this consultation stage impact assessment that manufacturers will incur a one off cost of redesigning their packaging, rather than opting for a stick on label. As the cost of redesigning packaging is a one off fixed cost, it is not expected that this will be passed onto consumers through higher prices.

Research has previously been conducted on labelling and packaging costs for changes to legislation regarding food labels. This is presented in the table below:

Table 5

Research	Author	Cost estimate for packaging redesign per Stock Keeping Unit (SKU)
Developing a framework for assessing the cost of labelling changes in the UK	Campden BRI for DEFRA 2010	Based on company size: £2,000-£4,000 Based on minor changes: £1,800 Average cost of redesigning due to legislation: £2,945
The introduction of mandatory nutrition labelling in the European Union. Impact assessment undertaken for DG SANCO	EAS (2004)	Based on minor changes: €2,000-€4,000

For the purpose of this impact assessment, it is assumed that the cost to manufacturers will be £3,000 on average per product, where producers redesign their external packaging.

We welcome further evidence on types of labelling and their respective costs as part of the consultation.

The following estimates are based on the assumption that UK manufacturers will incur a one off cost of redesigning their packaging, estimated to be £3,000 per product, which will not be passed onto consumers. This is because it is a one off cost, rather than an ongoing cost.

Therefore, it is also assumed that foreign manufacturers will not pass this cost on to UK consumers. However, if they should choose to use adhesive labels, there is a risk that the marginal cost may be passed on.

The cost of amending the label in the future, as a product's security changes, is deemed not to incur significant redesign costs. Moreover, it is impossible to predict the frequency with which this will occur.

The total cost to UK businesses of labelling has been calculated by multiplying the average cost of redesigning a label by the number of different IoT products produced in the UK. The cost to businesses will vary depending on the number of products that each firm manufactures.

As the IoT sector is still very young, there is a lack of data on the number of different IoT products on the market. Therefore, it has been assumed that the average number of consumer IoT goods produced per business is 6.[71] Sensitivity analysis has also been conducted with the lower and upper average estimate of 2 and 10 products per business, as well as £2,000 and £4,000 as the upper and lower estimates of cost of redesigning packaging per product.

As part of the consultation, we will welcome any further evidence on these assumptions.

Table 6: Estimation of labelling costs

	Best estimate (6 products/firm, £3,000)	Lower estimate (2 product/firm, £2,000)	Upper estimate (10 products/firm, £4,000)
Total cost to UK IoT manufacturers	£1,242,000	£276,000	£2,760,000

However, it should be taken into account that producers will always have packaging and labelling costs that are not associated with this regulation. The usual lifecycle of product packaging should also be considered, as any changes implemented as part of this lifecycle can be incorporated into the scheduled redesign, and reduce any additional costs.

This is likely to be the case for many businesses if there is a voluntary implementation period in which businesses have time to make changes to their packaging before the legislation comes into force. Initial engagement with industry has advocated for a minimum two year "grace period", where companies would be given sufficient time to plan for the proposed changes.

A RAND Europe survey found that 83% of food manufacturers change their packaging at least every 3 years.[72] Further, UK research has suggested that 80% of businesses in the food sector use up their stock of labels within 2 years, with smaller manufacturers taking longer than larger ones.[73] Many device manufacturers release upgraded versions of their

[71] This estimate comes from market research on a sample of the 69 businesses identified. It should be taken into account that a significant number of businesses provide IoT services and platforms rather than physical devices, so would not require a label.
[72] Assessing the impact of revisions to the EU nutrition labelling legislation, 2008, RAND Europe.
[73] Leatherhead Food International, Evaluating the impact on business chances to nutrition labelling requirements in the UK (Project undertaken for the Food Standards Agency, 2006).

products on an annual basis, leading to the design of new packaging, which can incorporate the DCMS security label.

Therefore, if there is a 3 year implementation period, it can be expected that these costs will be reduced by around 80%, resulting in a total cost to UK businesses of £248,400, which is comparable with the lower cost estimate.

Retailer Inspection Costs

This cost only applies to policy options A and C, where manufacturers are mandated to display a security label on their products. It is expected that warehouse staff will inspect a sample of incoming products to make sure that all relevant goods have a security label.

The number of retailers that will be affected is also difficult to estimate, as consumer IoT is sold across a range of sectors, for example supermarkets, health and fitness, hardware and domestic appliances, homeware, toys and other electrical stores. Further, many businesses that produce and sell IoT products do not identify themselves as IoT retailers or manufacturers. An estimate of the number of the potential number of consumer IoT retailers can be approximated using the ONS Business Population Estimates 2018. This estimates that the number of non-specialised stores, retailers of information and communication equipment in specialised stores and other household equipment in specialised stores in the UK is 48,060 employers.[74]

It can be assumed that product inspection will be included as part of general quality assurance checks of the products. This cost will vary across retailers, who stock different levels of consumer IoT products. DCMS does not currently have sufficient information to estimate the impact of this cost to retailers.

As part of the consultation, DCMS is looking to engage with retailers to learn more about the measures that will be taken in order to comply with the regulation. This includes additional costs of staff time and any other costs incurred, such as training.

Disposing of unsold legacy stock

It is expected that the cost of being unable to sell non-compliant stock after the voluntary transition period will be negligible. This is because it can be assumed that retailers will be able to plan to minimise stock losses by reducing the number of non-compliant products in the lead up to the regulation being enforced.

Cost to Government

The cost to government of implementing this regulation will involve monitoring costs. It has been assumed for the purposes of this consultation impact assessment that the enforcement agency will inspect a sample of consumer IoT goods before they reach UK retailers.

[74] Business Population Estimates for the UK and regions: 2018, Table 7, ONS, 2018.

Government funded bodies, such as Trading Standards, would be an option to carry out these duties. The median wage of a quality assurance and regulatory professional is £21.00 per hour.[75] DCMS will be considering different enforcement options as part of the consultation.

Manufacturers could also be randomly asked to provide evidence that the information stated on their label is accurate. DCMS plans to consult on the costs that monitoring will incur, and the most efficient method for this to be done. Therefore, the total cost of monitoring cannot yet be estimated, however, it is assumed that this will be a flat cost of the same magnitude for all options.

The Secure by Design team in DCMS has already published and promoted their Code of Practice for Consumer IoT, which this regulation will be based upon.

DCMS plans to consult on what monitoring and enforcement of the labelling scheme should involve and the costs that this will include.

Cost of Security Improvements

Under policy option A, improvements in product security are voluntary, however, under options B and C, they will be mandated.

There is currently a lack of data on the current level of security features in consumer IoT goods, however, the Internet of Things Security Foundation's report on vulnerability disclosure[76] found that around 90% of the 331 global IoT companies researched had no form of vulnerability disclosure mechanism.

Due to the lack of data on the current level of security in IoT products, and the cost that implementation will impose on manufacturers, the cost of amending existing product security features is currently unknown. DCMS is currently commissioning research in order to be able to calculate this cost.

The cost of security improvements will be estimated for options B and C using information gained from engagement with manufacturers, which is currently taking place. This will then be used to calculate the total cost to the 69 UK manufacturers that DCMS has identified by taking the marginal cost of security improvements per product multiplied by the proportion of devices that we estimate will improve in quality.

It can be assumed for policy option A, where security improvements are not mandated, that manufacturers will only amend their products where the benefit of doing so will exceed the costs. However, only once consumer preference shifts, and they start to buy more secure

[75] Annual Survey of Hours and Earnings (ASHE), ONS, 2017. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

[76] https://www.iotsecurityfoundation.org/best-practice-guidelines/

devices, will manufacturers be incentivised to amend their production processes to improve the security of IoT devices, as there is a profit incentive.

There is a risk that manufacturers may pass the cost on to consumers. Initially there will be a fixed cost of redesigning existing products, however there may be an increase in production costs if designing future products as secure imposes additional marginal costs.

The proportion of costs from voluntarily improving product security features passed onto the consumer will depend upon price elasticity of demand and the value placed on privacy and security relative to a product's other characteristics.

DCMS does not currently have sufficient information on the cost of complying with each of the 13 Code of Practice guidelines in order for an estimate of the costs to be made. We are currently carrying out research, and plan to investigate this further in consultation.

DCMS welcomes any further evidence on the cost to industry of implementing each of the 13 Code of Practice guidelines, as well as any evidence on the extent to which how many of the IoT products available on the market currently comply.

Cost to the secondary market

There will likely be a secondary effect on the used products market if companies/consumers who sell second-hand devices must also comply with the legislation. If we were to include this within scope for regulation, companies and consumers will be unable to re-sell any second-hand consumer IoT products without security labels on the packaging. This effect is currently unquantifiable but we will look to consult with stakeholders on this area before taking forward any further work.

As part of the consultation, we aim to investigate the cost to these businesses, and discuss policy options for implementing the regulation for this group. This may involve a longer implementation period, or excluding them from the scope of the regulation altogether.

Reputational Benefits to Business

The following analysis only applies to policy option A, as it is the only option where firms display a positive or negative label.

Businesses that display a positive security label on their product will benefit from consumers easily identifying their products, which demonstrate good practice in compliance with the identified Code of Practice controls. This signal to consumers may have reputational benefits, resulting in higher sales of safer products, resulting in higher profits for businesses with positive labels.

However, there is uncertainty around the impact of making improvements to insecure products, in order to comply with the Code and display a positive label, on prices and profits.

A Microsoft survey[77] found that security was a top priority for 17% of UK consumers, coming second only to value for money (19%). 25% assumed that their device was already secure, and 20% didn't know how to take action to secure their device. 77% of UK consumers surveyed said that they were willing to pay more for smart devices that already had security built in, whilst 93% said that they expect manufacturers to do more to secure smart devices.

Therefore, if it is assumed that consumers do care about their IoT device's level of security, businesses that demonstrate good practices will benefit from positive publicity. This may result in higher demand for their more secure product despite price increases, leading to higher profits.

Consumer Benefits

Consumers will be the main beneficiaries of the proposed regulation. There will be varying levels of benefit under each policy option.

The main benefit to consumers will be a reduction in the costs associated with IoT breaches through purchasing more secure devices, or taking action to secure insecure devices connected to their networks. Becoming more informed about their personal cyber security through mandating a labelling scheme, consumers may also be more likely to take action to increase the security of their existing products.

The full impact of the label will not be realised for a number of years after its initial implementation. This is due to the time that it takes for consumers to change their spending habits to incorporate the new information about security into their decision making process. There is a further lag in the time that it will take for consumers to disconnect the insecure devices that they already own from their home networks for the full benefit of increased awareness of cyber security to be realised.

This has been estimated through making assumptions about the reduction in cyber attacks as a result of the different policy options, continuing to use the assumption that, on average over the 10 year period, 5% of IoT devices are attacked per year (sensitivity analysis undertaken using 1% and 10% for lower and upper estimates).

According to the 10th annual Verizon Data Breach Investigations report, 81% of hacking related breaches involved stolen or weak passwords.[78] Hence, under option A and B, where safer devices will have implemented 3 of the CoP guidelines, it has been assumed that there could be a 40% reduction in the incidence of breaches (sensitivity analysis: 10% and 50%). This assumption increases to 60% under option C, where all 13 guidelines are implemented (sensitivity analysis: 20% and 70%).

There is a lack of robust evidence around this assumption, as this Government-led intervention has not been trialled anywhere in the world. Therefore, we have used wide

[77] A Consumer take on smart device security, Microsoft Azure, 2019.
[78] 2017 Data Breach Investigations Report, Verizon.

ranges in our sensitivity analysis to account for the uncertainty around the potential benefits. This assumption is the main driver of the variance in benefits across policy options.

We have also made assumptions about the rate at which consumers update their IoT devices. These assumptions are based on research by PWC, which found that over 40% of consumers are expected to update their IoT home devices within the next 2 years.[79] It has, therefore, been assumed that under policy options B and C, where improvements to device security are mandated, ownership of compliant consumer IoT devices will increase at an annual rate of 20%. As a result, after 5 years all consumer IoT devices in the UK would comply with the 3 CoP guidelines.

However, some consumers may take longer before upgrading their devices, while some may not upgrade at all. We do not have sufficient evidence to model this and so it has been assumed that these consumers do not make up a significant proportion of the population.

Benefits to consumers will also depend upon the rate of adoption of the more secure devices. Under policy option A, with a positive or negative label, it is assumed that 15% of consumers will switch to a device with a positive label. Under policy options B and C, all devices must be made more secure, so everyone with a new device will benefit from better security.

Table 7: Consumer benefit scenario analysis assumptions

Assumptions	Best Estimate	Low Estimate	Upper Estimate
% of devices attacked	5%	1%	10%
Policy option A and B: reduction in probability of attack	40%	10%	50%
Policy option C: reduction in probability of attack	60%	20%	70%

Low estimates are calculated assuming that 1% of devices will be attacked, and that there will be a (10%)/(20%) reduction in probability of attack for policy options (A and B)/(C). Upper estimates are calculated assuming that 10% of devices will be attacked, and that there will be a (50%)/(70%) reduction in probability of attack for policy options (A and B)/(C). Best estimates are calculated assuming that 5% of devices will be attacked, and that there will be a (40%)/(60%) reduction in probability of attack for policy options (A and B)/(C).

Wider impact

Mandating manufacturers to make products more secure will reduce the number of IoT vulnerabilities in UK economy. As a result, fewer devices could be used in DDoS attacks.

[79] Connected Home 2.0, PWC, 2018.

However, as these attacks are not geographically limited, this is a global problem, which cannot be resolved through unilateral action.

Under policy option A, manufacturers may be incentivised to make IoT products more secure in response to the compulsory labelling legislation. This should have the effect of reducing the number of vulnerabilities in IoT devices in the UK, leading to a more secure ecosystem. This will bring benefits to society as a whole, such as a reduction in the impact of cyber-attacks, for example DDoS attacks that use insecure devices and can affect consumer services and vital infrastructure.

Labels have previously been an effective market lever in incentivising manufacturers to improve the quality of their products. Improvements in the energy efficiency of white goods, since the introduction of the efficiency label, have led to the label's categories being updated in order for consumers to be able to differentiate between the best performing goods.[80]

This benefit is expected to be greater under policy options B and C, where manufacturers are mandated to make products more secure. However, it is difficult to quantify the impact, due to the lack of a counterfactual and the unpredictability of the frequency and cost of large scale DDoS attacks.

Option A - Analysis of Costs

Cost to businesses

Familiarisation costs

Costs will be incurred by businesses as they familiarise themselves with the legislation and its implications for their firm. This analysis estimates the impact to IoT manufacturers operating in the UK, of which 69 have been identified.

We assume that, on average, it will take one manager 30 minutes to familiarise themselves with the regulation, as guidance documents have previously been provided by the government and produced by industry. This is in line with the Food Labelling impact assessment published in 2018.[81] It is also assumed that businesses will employ a legal professional, who will take 30 minutes to familiarise themselves with the legislation.

Table 8: Familiarisation costs

	Best estimate (median)	Lower estimate (20th percentile)	Upper estimate (80th percentile)
Cost per business	£41.74	£25.20	£61.01

[80] Johnson, S.D., Blythe, J.M., Manning, M., and Wong, G. (2019). The impact of IoT security labelling on consumer product choice and willingness to pay. Submitted for peer review

[81] Impact assessment: mandating energy labelling of food and drink in out-of-home settings, Department for Health and Social Care, 2018.

Total cost	£2,880.27	£1,738.83	£4,209.62

Self assessment costs

This cost stems from initially identifying the information required to put on the label, as part of the self-certification process. This will be a one-off cost per product, unless the manufacturers choose to redevelop the specifications of an existing product.

We estimate that it will require 30 minutes to identify and evidence the information on the three CoP guidelines that will be used to determine the label per product. This is then multiplied by the median hourly wage of a planning, process and production technician, which is estimated to be £15.67 from the ASHE 2017.

Sensitivity analysis has been conducted using the 20th and 80th percentile hourly wages of a planning, process and production technician, as well as the assumption for the average number of products per manufacturer of 2, 6 and 10. Any additional evidence on this assumption would be welcomed.

As part of the consultation, DCMS would like to know, on average, how often existing IoT products are redeveloped, how many new products IoT manufacturers produce per year, as well as the average number of products per manufacturer.

Table 9: Self-certification costs

	Best estimate	Lower estimate	Upper estimate
Total cost	£3,243.69	£847.32	£6,561.90

Labelling costs

DCMS' current estimate of the total cost to the sector of redesigning packaging is £1,242,000. However, with the introduction of a 3 year implementation period, this cost could decrease to £248,400.

Cost to retailers

Inspection costs

As previously stated, inspection costs will likely be incorporated into existing quality assurance processes and therefore, the cost is expected to be small. Retailers may also incur costs of training staff to inspect products that they stock in order to ensure that they have the appropriate labels on.

Cost of disposing of legacy stock

It is expected that the cost of disposing of non-labelled stock after the voluntary transition period will be negligible.

Indirect cost of security improvements

A secondary impact of option A is if manufacturers choose to redesign their products in order to be able to present a positive label on their packaging. The proportion of costs from voluntarily improving product security features passed onto the consumer will depend upon price elasticity of demand and the value placed on privacy and security relative to a product's other characteristics.

There is a risk that at least part of the improvement costs will be passed onto the consumer, which may lead to lower sales of products that go through the improvement process, resulting in lower profits. However, as improving the security of consumer IoT products will remain voluntary under this policy option, it is expected that businesses would only do this where the benefits of doing so outweigh the costs. DCMS is currently conducting research on the cost of implementing the 3 CoP guidelines and whether this cost will be passed onto consumers.

Cost to consumers

It is not expected that there will be a significant cost to consumers from implementing a mandatory label, as it is a one off initial cost.

However, there is a risk that the cost of manufacturers implementing security improvements to their products will be passed on to consumers. This is a secondary effect, as it is not mandated by policy option A, so will depend on the number of manufacturers that amend their production processes and the cost that this will impose on businesses.

There will be a small time cost to consumers of processing the information on the label and accounting for this when making purchasing decisions, however, this is negligible.

Cost to government

There will be a cost to government of monitoring, to ensure that manufacturers comply with the specifications of the labelling scheme. Government funded bodies, such as Trading Standards, would be an option to carry out these duties. DCMS will be considering different enforcement options as part of the consultation. This is assumed to be a flat cost across all three policy options.

Option A - Analysis of Benefits

Benefits to consumers

The main benefit to consumers of mandating a security label will be to reduce information asymmetry, so that the level of security of consumer IoT products can easily be identified at the point of purchase. As a result, this could lead to consumers experiencing fewer breaches.

Studies on food labelling awareness show that where consumers check nutrition information on packaging, the majority of consumers are able to identify healthier choices, particularly among those who had prior knowledge.[82] A link has also been identified between nutrition knowledge and label use.[83] Research on the proportion of consumers who use labelling information to make healthier food choices is summarised in the table below:

Table 10

Title	Author	Findings
Impact of food labelling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies. Obesity Reviews, 17: 201–210.	2016, Cecchini, M., and Warin, L.	Food labelling would increase the amount of people selecting a healthier food product by about 17.95% (confidence interval: +11.24% to +24.66%).
Study on the Impact of Food Information on Consumers' Decision Making	2014, TNS European Behaviour Studies Consortium	Calorie labels led to 16% of consumers planning to reduce alcohol consumption on a specified occasion.This was less effective on those who weren't interested in health. A 'Know your limits' label led to a 19% planned decrease on specified occasion. Long term willingness to reduce consumption by 17%.

It is therefore assumed for the purposes of this consultation impact assessment that 15% of consumers will switch to more 'secure devices' on average over the 10-year period, as a result of the label in option A . This may be an under-estimate, however, as consumers may be more likely to change their behaviour upon being made aware of the relative security

[82] Study on the Impact of Food Information on Consumers' Decision Making, TNS European Behaviour Studies Consortium, 2014.
[83] The effects of nutrition knowledge on food label use. A review of the literature, Miller, L., Cassidy, D., University of California, 2015.

risks of IoT purchases than they are in response to nutritional information. DCMS welcomes any further evidence on these assumptions.

As a result of this behavioural change, it can be assumed that these consumers will have greater protection against cyber attacks than their peers. It has been assumed that, on average, 5% of IoT devices will be attacked per year (sensitivity analysis: 1% and 10%). It has also been assumed that there could be a 40% reduction in the incidence of breaches (sensitivity analysis: 10% and 50%). The benefit to consumers can, therefore, be estimated by multiplying the expected reduction in cost to individuals of an attack by the predicted number of 'secure devices'.[84]

Table 11: Estimated benefits to consumers: Present Value

Best Estimate (5%/40%)	Lower Estimate (1%/10%)	Upper Estimate (10%/50%)
£363,100,000	£18,200,000	£907,900,000

However, it must be taken into account that these are simplifying assumptions, and that consumers will not be protected against all attacks by purchasing products with a security label.

Table 12: Cost-benefit summary: Option A

Group Affected	Impact	Present Value (£)
Businesses	Familiarisation costs	£2,880
	Self-certification costs	£3,243
	Labelling costs	£1,242,000
	Cost to secure products	Unquantified
	Cost to retailers	Unquantified
	Disposing of legacy stock	0
	Cost to secondary market	Unquantified
	Change in profits	Unquantified
	Total Business Costs	£1,248,123
Government	Monitoring	Unquantified
	Total Costs	£1,248,123

[84] Predicted number of 'secure devices' is estimated by using the assumption that 15% of devices (using the forecast of number of IoT devices), on average over the 10 year period, are switched to those that comply with the 3 CoP guidelines. This is then used to calculate the estimated benefit to consumers through expected reduction in the cost of attacks (No.devices*15%*5%*£271*40% accumulated over the 10 year period taking into account the forecasted growth rate in IoT devices).

Consumer	Consumer security benefits	£363,100,000
Wider Society	Security benefits	Unquantified
	Total Benefits	£363,100,000
	Net Present Value	£361,900,000

Option B - Analysis of Costs

Cost to businesses

Familiarisation costs

There will be costs to manufacturers to familiarise themselves with the three Code of Practice Guidelines that the legislation enforces. It is expected that it will require more time to familiarise with the legislation compared to option A, as technical changes will have to be made in order to comply with the regulation.

The total cost to the sector of familiarisation is expected to be £5,760. This includes the 1 hour time cost of both senior managers and legal professionals.

Table 13: Familiarisation costs

	Best estimate (median)	Lower estimate (20th percentile)	Upper estimate (80th percentile)
Cost per business	£83.49	£50.40	£122.02
Total cost	£5,760.53	£3,477.67	£8,419.24

The wages for the Legal professional and Information technology and telecommunications directors are taken from the ONS's ASHE 2017. The median is used as a best estimate, as it is believed to be the most representative wage (it's less skewed by outliers). Overhead charges of 30% are added to the wages, in accordance with the International Standard Cost Model Manual.

Self assessment costs

Self-certification requires firms to initially identify whether their product complies with the regulation, and later compile evidence to prove that it does. We estimate that it will require 30 minutes to identify the information that will be used to evidence that devices are compliant with the three Code of Practice Guidelines. This is then multiplied by the median hourly wage of a planning, process and production technician, which is estimated to be £15.67 from the ASHE 2017.

This is the same as option A, as they both require evidence on the same 3 identified CoP guidelines.

Table 14: Self assessment costs

	Best estimate	Lower estimate	Upper estimate
Total cost	£3,243.69	£847.32	£6,561.90

Cost of security improvements

Individual businesses will be affected differently by mandating that manufacturers must meet the three standards identified in the Code of Practice. This may also involve ensuring that component parts from their suppliers comply with the regulations. There is a risk that at least part of the improvement costs will be passed onto the consumer.

Some businesses may already comply with some, or all of the specified standards, while for others it may be too costly to redesign their products in order to comply. This could result in some manufacturers going out of business.

DCMS does not currently have sufficient information on the cost of complying with the Code of Practice guidelines in order for an accurate estimate to be made.

Cost to Government

There will be a cost to government of ensuring that manufacturers are meeting the specified minimum security standards. Government funded bodies, such as Trading Standards, would be an option to carry out these duties. DCMS will be considering different enforcement options as part of the consultation. This is assumed to be a flat cost across all three policy options.

Option B - Analysis of Benefits

Consumers

Consumers will benefit from enforcing the three Code of Practice Guidelines, as their IoT devices will become more secure. However, it will take time for the full impact to be realised, as consumers will still be vulnerable to attacks with even one insecure device connected to their network. Therefore, consumers will only become more secure once all of the products in their home have been replaced.

Unlike mandating a label, consumers will not become more aware of the security of their IoT products, so are less likely to take action themselves to secure their pre-existing devices. This will limit the benefits of securing consumer IoT devices in the short run.

The main benefits of consumers becoming more secure, through mandating the three guidelines, will be the reduction in breach related costs to consumers. The benefit of reducing these costs are difficult to quantify, due to the lack of available data on the incidence of cyber attacks against personal IoT devices.

It has been assumed that, on average, 5% of IoT devices will be attacked per year (sensitivity analysis: 1% and 10%). It has also been assumed that there could be a 40% reduction in the incidence of breaches (sensitivity analysis: 10% and 50%). This will apply across all devices which comply with the regulation. It is also assumed that the rate of adoption will increase annually by 20% for the first 5 years, until 100% of devices owned in the UK are secure.

Consumers will be less aware of their security under this policy option because no label is mandated, as all products must comply with the regulation. Therefore, consumers may not take action to secure their existing devices, of which they do not know whether they comply with the regulation.

This policy option may lead to higher levels of security in the long run versus option A, as all products must comply with the three Code of Practice Guidelines. However, the lack of consumer awareness means that consumers will not take further precautions to protect themselves and the insecure products that they currently own in the short run.

Table 15: Estimated benefits to consumers: Total Present Value

Best Estimate (5%/40%)	Lower Estimate (1%/10%)	Upper Estimate (10%/50%)
£2,052,400,000	£102,600,000	£5,131,100,000

Table 16: Cost-benefit summary: Option B

Group Affected	Impact	Present Value (£)
Businesses	Familiarisation costs	£5,760
	Self-certification costs	£3,243
	Cost to secure products	Unquantified
	Total Business Costs	£9,003
Government	Monitoring	Unquantified
	Total Costs	£9,003
Consumer	Consumer security benefits	£2,052,400,000
Wider societal	Security benefits	Unquantified
	Total Benefits	£2,052,400,000

Net Present Value	£2,052,391,997

Option C - Analysis of Costs

Cost to businesses

Familiarisation costs

The regulatory burden placed on manufacturers is greater under option C, compared to both A and B. This is because manufacturers will have to produce a label, as well as redesign their products in order to comply with all 13 CoP guidelines. Therefore, it is expected that it will take more time for businesses to familiarise with the guidance and regulation documents.

DCMS is planning to consult with industry further on the cost of familiarisation, however for the purpose of this estimate, it is expected that this will require 2 hours of a manager's time and 1 hour of a legal professional's time.

Table 17: Familiarisation costs

	Best estimate (median)	Lower estimate (20th percentile)	Upper estimate (80th percentile)
Cost per business	£113.84	£68.30	£173.02
Total cost	£7,855.03	£4,712.84	£11,938.17

Self assessment costs

There will also be a greater administrative burden on manufacturers to provide evidence as part of the self-certification process under option C, as they will have to comply with a greater number of guidelines. DCMS estimates that it will take a planning, process and production technician on average 2 hours to evidence that their product is compliant with all 13 of the CoP guidelines. Any further evidence on this assumption would be welcomed.

Table 18: Self-certification costs

	Best estimate	Lower estimate	Upper estimate
Total cost	£12,974.76	£3,389.28	£26,247.60

Cost of security improvements

The cost for manufacturers of complying with all 13 guidelines in the Code of Practice, as well as producing a label, will place a disproportionate burden on manufacturers, especially small and micro businesses.

Individual businesses will be affected differently by mandating that manufacturers must meet the Code of Practice standard. This may also involve ensuring that component parts from their suppliers comply with the regulations.

In order to achieve this standard of security, many products would have to be completely redesigned in order to be sold to UK consumers. Some businesses may already comply with some, or all of the specified standards, while for others it may be too costly to redesign their products in order to comply. This could result in some manufacturers going out of business.

Compliance with the regulation could also result in ongoing costs to manufacturers through embedding the secure by design policies into the product development process. As the burden on manufacturers of complying with all 13 guidelines is much greater than policy option B, it is expected that these increased production costs could be passed onto the consumer through higher prices.

DCMS does not currently have sufficient information on the cost of complying with all 13 Code of Practice guidelines in order for an estimate to be made. We are currently carrying out research on the cost to businesses, but plan to investigate this further in consultation.

Labelling costs

DCMS believes that it is essential for consumers to be aware of the security features of the products that they are purchasing, to provide assurance that the product that they are buying is deemed to have the appropriate level of security. As all goods sold in the UK will be required to comply with the regulation, only positive labels will be displayed.

The cost of labelling will be the same as under policy option A. As this will be a one off cost, it is not expected that packaging redesign costs will be passed on to UK consumers from foreign manufacturers.

DCMS' current estimate of the total cost to the sector of redesigning packaging is £1,242,000. However, with the introduction of a 3 year implementation period, this cost could decrease to £248,400.

Cost to consumers

Domestic and foreign manufacturers may pass on their increased production costs to UK retailers as a result of increasing their product security. As previously mentioned, the extent to which these costs are passed onto UK consumers is currently unknown. However, as the cost of compliance with this option will be greater, the impact on prices can also be assumed to be greater.

As a result, this may have distributional consequences, as the cost of IoT goods will represent a larger proportion of individual incomes. The impact on businesses may also lead to a reduction in consumer choice, which could limit competition and cause prices to increase.

Cost to government

Government may have to provide more guidance and support under policy option C, due to the greater burden that is being imposed on manufacturers. The Secure by Design team in DCMS has already published and promoted their Code of Practice for Consumer IoT, which this regulation will be based upon.

There will be a cost to government of ensuring that manufacturers are meeting the specified minimum security standards. Government funded bodies, such as Trading Standards, would be an option to carry out these duties. DCMS will be considering different enforcement options as part of the consultation. This is assumed to be a flat cost across all three policy options.

Option C - Analysis of Benefits

Consumers

In the long run, the reduction in the cost of breaches, as consumers buy more secure devices, is expected to be larger than option A or B as all devices must comply with all 13 CoP guidelines. This impact may take longer to be realised compared to previous options, as if devices become more expensive, consumers will replace their insecure devices with secure ones at a slower rate.

However, as DCMS does not currently have evidence on the extent of the change in prices as a result of increasing costs of production, and hence the effect on consumer behaviour, the rate of adoption of safer devices is assumed to be the same as under option B. This could lead to an overestimate of the benefits under this option.

It has been assumed that there could be a 60% reduction in the incidence of breaches (sensitivity analysis: 20% and 70%). This is greater than previous options, as consumer IoT products will have a higher level of security, through mandating all 13 of the CoP guidelines.

Table 19: Estimated benefits to consumers

Best Estimate (5%/60%)	Lower Estimate (1%/20%)	Upper Estimate (10%/70%)
£3,078,700,000	£205,200,000	£7,183,500,000

Table 20: Cost-benefit summary: Option C

Group Affected	Impact	Present Value (£)
Businesses	Familiarisation costs	£7,855
	Cost of self-certifying	£12,974
	Labelling costs	£1,242,000
	Cost to secure products	Unquantified
	Cost to secondary market	Unquantified

	Change in profit	Unquantified
	Total Business Costs	£1,262,829
Government	Monitoring	Unquantified
	Total Costs	£1,262,829
Consumers	Consumer security benefits	£3,078,700,000
Wider Society	Security benefits	Unquantified
	Total Benefits	£3,078,700,000
	Net Present Value	£3,077,400,000

The benefit of this option is not deemed to be proportionate to the cost of implementing the policy. It will cause a disproportionate level of disruption in the market and could result in unintended consequences for consumers through higher prices and less choice.

Equivalent Annual Net Direct Cost to Business & Business Impact Target

We will be looking at evidence that is collected at consultation stage to further inform this section.

Direct costs determined to be in scope are:

- Administration costs for manufacturers (familiarisation with the amended regulations)
- Costs to manufacturers of putting label on products
- Costs to manufacturers to self certify
- Costs of manufacturers amending development processes to meet requirements
- Cost to retailers of inspecting their stock

Using the Department for Business, Energy and Industrial Strategy Impact Assessment Calculator[85], the provisional Equivalent Annualised Net Direct Cost to Business (EANDCB) of the preferred policy option A is set out in the table below, alongside the Business Net Present Value and Business Impact Target Score.

Table 20: Provisional EANDCB and Business Net Present Value (£m)

	Policy option A	Policy option B	Policy option C
Equivalent Annualised Net Direct Cost to Business (EANDCB) - 2017 Prices	£0.1m	£0	£0.1m
Business Net	-£1m	£0	-£1m

[85] https://www.gov.uk/government/publications/impact-assessment-calculator--3

Present Value - 2017 Prices			
Score against the Business Impact Test	0.6	0	0.6

These costs are underestimated, as DCMS does not currently have the relevant data in order to estimate the cost to manufacturers of amending their production process in order to comply with policy options B and C. These costs will be estimated after the consultation in the full impact assessment.

Specific Impact Tests

Assessment of Impact on Competition

The impact of the proposed regulation can be assessed through its expected effect on competition.

Manufacturers who do not comply with the regulations by displaying a security label on their product will be excluded from the market. This may create an additional barrier to entry for new companies wishing to enter the market.

All firms producing consumer IoT products will be affected by the regulation, however, larger companies may face higher costs as they have a wider range of products and sell more devices. There is a small risk that the cost of adopting the label may lead to some firms going out of business, however this cost is unlikely to be prohibitively expensive for existing businesses.

It may be more likely in the long run that business closures are caused by a reduction in sales due to reputational damage caused by displaying a negative label. Where it is too expensive for the manufacturer to improve the product's safety and security, firms may in the long run leave the market.

In any affected market, would the proposal:

1. Directly limit the number or range of suppliers?

The proposed regulation will limit the range of suppliers, as those who do not display the cyber security label will not be able to sell their product in the UK. In order to display the label, they must go through a self-certification process which decides whether a positive or negative label can be displayed.

Manufacturers may decide not to sell to the UK market as a result of the regulation, which would limit consumer choice and competition.

2. Indirectly limit the number or range of suppliers?

All suppliers will face the same labelling costs, however manufacturers will always face packaging costs unrelated to their product's security. Those who display a negative label, as they are not in compliance with the three identified Code of Practice guidelines, may be at a disadvantage to their competitors who display a positive label.

The label will also impose a small additional cost, due to the self-certification process, which could create an additional barrier to entry for new businesses, however this is likely to be insignificant.

3. Limit the ability of suppliers to compete?

The proposed regulation will not mandate that suppliers change their production process, only that they signal to consumers the level of basic security that their product has. There is no minimum standard required in order to sell the product, other than the use of the security label.

4. Reduce suppliers' incentives to compete vigorously?

It is expected that the provision of the label will result in competition based on product security features, as this information is not currently easily available and comparable for consumers when making purchasing decisions.

We will be looking at evidence that is collected at consultation stage to further inform this section.

Under policy options B and C, the cost of redeveloping some low cost products may exceed the value of the good itself, resulting in some firms going out of businesses and some products no longer being available on the UK market.

As a result of these options, there may be a reduction in competition, giving large firms who are more able to meet the minimum standard a competitive advantage. Compliance with all 13 of the IoT Code of Practice guidelines will create a further barrier to entry for UK IoT firms. This could stifle innovation in the UK technology sector, due to the high level of regulation in comparison to the rest of the world, resulting in lower levels of investment into the growing IoT market.

Small and Micro Business Assessment

This section estimates the costs to small and micro businesses in the UK. We will be looking at evidence that is collected at consultation stage to inform this section, including quantifying the impact on profits of small and micro firms.

DCMS plans to consult further on figures for the number of consumer IoT manufacturers in the UK, broken down by their size. Of the 69 UK based IoT manufacturers identified, 21 were classified as micro, and 27 as SMEs.

The IoT supply chain is young and developing, with new products emerging from a wide array of start up companies both within the UK and globally. Therefore, we do not deem it appropriate to exempt businesses from the regulation as they too have an impact on the IoT consumer market.

From these estimates, small and micro businesses make up approximately 70% of the consumer IoT market in the UK, as it is a growing and emerging industry. Using the IoT Nation database, we have identified that there are approximately 48 small and micro businesses in the UK that are producing consumer IoT devices (21 micro, 27 SME, 12 unknown).[86]

Impact on small businesses

- Familiarisation
- Labelling costs
- Self-certification
- Improvements to product security (currently unquantified)

We expect that the regulation will have a disproportionate impact on small and micro businesses, as the initial fixed cost of compliance will represent a greater proportion of their revenue, compared to medium and large businesses. There is a risk that the burden of regulation could force some small and micro businesses to leave the market. However, the implementation period will help to reduce these costs by giving small and micro businesses longer to adjust.

We have assessed the impact of the following costs to small and micro businesses for policy option A (the preferred option):

	Micro (n=21)	Small (n=27)	All firms (n=69)
Familiarisation cost	£864.08	£1,123.31	£2,880.27
Self-certification cost	£973.11	£1,265.04	£3,243.69
Labelling cost	£372,600	£484,380	£1,242,000

There is a lack of evidence for how these costs would vary by business size. For micro and small businesses it is assumed that familiarisation costs will be a greater burden than for medium and large businesses, as they have fewer available resources to manage the change in regulations.

[86] https://iotuk.org.uk/projects/iotuk-nation-database%E2%80%8B/

However, SMBs are likely to have a smaller range of IoT products than large enterprises, so the cost of self-certifying and redesigning packaging will be lower in comparison.

Some small and micro businesses, which may not be captured in the 69 UK manufacturers identified, may be part of the supply chain of larger firms producing consumer IoT goods. These businesses in the supply chain, who are involved in the security vulnerability lifecycle management, will likely see a cost in terms of resource costs.

As a result of the regulation, these suppliers may be required to provide information on the security of the component parts that they provide in order for the manufacturer to design the label. Therefore, they may also face administrative reporting costs. However, due to the complexity of supply chains, DCMS does not currently have sufficient information to be able to quantify this effect.

It could be assumed that small and micro firms may take longer to adjust to the regulation, as they have a smaller workforce and less specialised labour. It is unclear whether there will be a different response to introducing the label than medium and large enterprises. However, they may respond more quickly in terms of improving their products to comply with the Code of Practice, as they are building their reputation so would aim to avoid bad publicity associated with a negative label. They will also have fewer products that they would need to redevelop.

The labelling scheme will initially be voluntary for all businesses, to give manufacturers enough time to adjust their practices before the legislation passes and the label becomes mandatory. We will be able to give a better indication of how long the transition period will be once the estimated date for Primary Legislation to receive royal assent has been agreed.

There will be a greater cost burden on small and micro businesses under policy options B and C, which require products to adhere to minimum standards. These costs would fall specifically within the development process, amending production lines to support provisioning of devices and more specific additional support costs e.g. users who need extra support.

DCMS plans to further investigate the impact on small and micro businesses during the consultation, and possible options for mitigating costs for these businesses.

Risks and uncertainties

The impacts of the new regulations are uncertain due to a range of factors. The main factors identified are:

- There is a possible cost burden to consumers, as producers could raise product prices to account for the cost of adopting the label and optionally amending their production line. This scenario would result in products being more expensive, which would disproportionately affect lower income individuals (as consumer IoT costs a greater proportion of their disposable income leading to negative distributional effects) and the secondary market being affected (e.g. charity shops not being able to sell pre-owned consumer IoT that don't have a label).
- There will also be a cost to Government, or the appropriate enforcement agency, to monitor compliance and undertake enforcement to ensure that non-conformant devices (i.e. those without a label as set out in Option A, or those that do not comply with the top 3 guidelines in option B) are prevented from entering the market. Government will need to set out clear roles and responsibilities concerning enforcement, alongside a relevant new or existing framework that explicitly states what the consequences of non-compliance will be to industry. Where there isn't a robust enforcement landscape in place, there will always be the risk that a minority of companies will go undetected.
- There is also uncertainty around how consumers will react to the label. If consumers were to utilise label and as a result change their purchasing habits, the labelling scheme would have been successful in informing consumers to the vulnerabilities presently in consumer IoT devices.
- Moreover, this behaviour change should incentivise manufacturers to produce more secure devices, which will further benefit society in reducing the number of vulnerable devices on the market. However, these two effects depend upon the actions of the consumer in response to the information conveyed on the label.
- It will take time for the full impact of the regulation to be realised, as benefits accrued from creating a safer IoT ecosystem will increase over time as consumers update their existing, insecure products and replace these with those that comply with the three Code of Practice controls.

We will look to use the consultation period to consult with a range of stakeholders to seek clarification on the above risks and uncertainties.

Annex A: Code of Practice for Consumer IoT Security

https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

As we connect more devices in our homes to the internet, products and appliances that have traditionally been offline are now becoming part of the 'Internet of Things' (IoT).

The IoT represents a new chapter of how technology becomes increasingly common in our homes, making people's lives easier and more enjoyable. As people entrust an increasing amount of personal data to online devices and services, the cyber security of these products is now as important as the physical security of our homes.

The aim of this Code of Practice is to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world.

The Code of Practice brings together, in 13 outcome-focused guidelines, what is widely considered good practice in IoT security. It has been developed by the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), and follows engagement with industry, consumer associations and academia. The Code was first published in draft in March 2018 as part of the Secure by Design report.

The first three guidelines are prioritised because action on default passwords, vulnerability disclosure and security updates will bring the largest security benefits in the short term. The supporting text articulates the rationale and adds further detail for each guideline. Additional explanatory notes at the end of the document answer frequently asked questions.

Guidelines

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimise exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected

Annex B: Secure by Design background

This work is being taken forward as part of the Government's National Cyber Security Strategy (2016-2021) which outlines the Government's cyber security ambition over a five year period.[87]

The Secure by Design Review commenced in early 2017. The focus has been the development of a 'Code of Practice' for those developing, operating and selling IoT services and solutions, including device manufacturers. The Code of Practice sets out practical steps to improve the cyber security of consumer IoT products and connected services. It brings together what is widely considered good practice and applies it to the area of consumer IoT in the form of 13 guidelines.

Over the course of the Review, the Government has sought input from a range of stakeholders, including industry, academia, consumer bodies, other Government departments and international governments. In support of a multi-stakeholder advisory approach, the Government set up an independently chaired Expert Advisory Group which included a wide range of external stakeholders, including industry representatives, to support the review by advising and commenting on proposals for further action.

The Review comprised of three key strands of work, focusing on:

- Understanding the burden currently placed on consumers (ie. the expected behaviours when buying, installing, maintaining and disposing of a consumer IoT product);
- Developing guidelines for a secure by design approach in the form of a Code of Practice; and
- Broader Government incentives and levers to gain traction with industry.

Alongside a much broader set of cross government activities, this Review is intended to support both the UK's ambition to be a world-leading cyber security authority, and a prosperous and thriving digital economy.

[87] UK National Cyber Security Strategy, 2016, accessed at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Annex C: Counterfactual and policy overlaps

How the Code of Practice aligns with current regulations, reporting and security requirements

DCMS have undertaken a mapping of the current regulatory landscape. There are a number of existing regulations and requirements that align with specific guidelines within the Code of Practice - these are set out in full below.

General Data Protection regulation (GDPR)

The Data Protection Act 2018 and GDPR replaced the existing Data Protection Act (1998) in May 2018. This has strengthened the existing regulation and require reporting of all breaches of security that results in the loss, corruption or release of personal data to the Information Commissioner's Office (ICO).

There are a number of guidelines within the current Code of Practice that align with existing data protection legislation.

Guideline	How text within guideline aligns with GDPR
4: Securely store credentials and security-sensitive data *Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers*	Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable. Reverse engineering of devices and applications can easily discover credentials such as hard-coded usernames and passwords in software. Simple obfuscation methods also used to obscure or encrypt this hard-coded information can be trivially broken. Security-sensitive data that should be **stored securely** (GDPR Article 5(1)(f) applies) includes, for example, cryptographic keys, device identifiers and initialisation vectors. **Secure, trusted storage mechanisms should be used** (GDPR Article 32(1)(a)) such as those provided by a Trusted Execution Environment and associated trusted, secure storage.

5: Communicate Securely	Security-sensitive data, including any remote management and control, **should be encrypted** (Article 32(1)(a)) in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.
Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers.	The use of open, peer-reviewed internet standards is strongly encouraged. (GDPR Article 32)
8: Ensure that personal data is protected	Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the **General Data Protection Regulation (GDPR)** and the Data Protection Act 2018.
Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers, Retailers	Device manufacturers and IoT service providers shall **provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes** (GDPR Article 12(1)), for each device and service. This also applies to any third parties that may be involved (including advertisers). Where **personal data is processed on the basis of consumers' consent** (GDPR Article 6(1)(a)), this shall be validly and lawfully obtained, with those consumers being given the **opportunity to withdraw it at any time** (GDPR Article 17(1)(b)). This guideline ensures that: i) IoT manufacturers, service providers and application developers **adhere to data protection obligations** when developing and delivering products and services (GDPR); ii) **Personal data is processed in accordance with data protection law** (GDPR Article 5 (1)(f));

iii) Users are assisted in assuring that the **data processing operations of their products are consistent** (GDPR Article 25(1)) and that they are functioning as specified;

iv) Users are provided with means to preserve their privacy by configuring device and service functionality appropriately.

9: Make systems resilient to outages

Outages of networks or of power can happen**. Resilience should be built in to IoT services where required (GDPR Article 32 (1)(b))** by the usage or other relying systems**.**

Primarily applies to: Device Manufacturers, IoT Service Providers

As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. This includes ensuring that devices are able to return to a network in a sensible state and in an orderly fashion rather than in a massive scale reconnect.

IoT systems and devices are relied upon by consumers for increasingly important use cases that may be safety relevant or life-impacting. Keeping services running locally if there is a loss of network is one of the measures that can be taken to increase resilience. Other measures may include building redundancy into services as well as mitigations against DDoS attacks.

The level of resilience necessary should be proportionate and determined by usage but consideration should be given to others that may rely on the system, service or device as there may be a wider impact than expected.

10: Monitor system telemetry data

If telemetry data is collected from IoT devices and services, such as usage and measurement data, it **should be monitored for security anomalies** (GDPR Article 32(1))**.**

Primarily applies to: IoT Service Providers	Monitoring telemetry, including log data, can be useful for security purposes. It may allow for unusual circumstances to be identified early and dealt with, minimising other security risks and allowing quick mitigation of problems. In accordance with Guideline 8, however, the processing of personal data should be kept to a minimum and **consumers shall be provided with information about what data is collected and the reasons for this.**(GDPR Article 12(1))
11: Make it easier for consumers to delete their personal data *Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers*	Devices and services **should be configured** (Article 6(1)(a) or Article 6(1)(b)) such that personal data can easily be removed from them when there is a transfer of ownership, When the **consumer wishes to delete it** (GDPR Article 17(1)) and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.
12: Make installation and maintenance of devices easy *Primarily applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers*	Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device. Security issues caused by consumer confusion or misconfiguration can be reduced and sometimes eliminated by properly addressing complexity and poor design in user interfaces. **Clear guidance to users on how to configure devices securely** can also reduce their exposure to threats. (GDPR Article 12(1))

13: Validate input data	Data* input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.
Primarily Applies to: Device Manufacturers, IoT Service Providers, Mobile Application Developers	This **can be subverted by incorrectly formatted data or code transferred across different types of interface**.(GDPR Article 5(1)) Automated tools are often employed by attackers in order to exploit potential gaps and weaknesses that emerge as a result of not validating data. Examples include, but are not limited to, data that is: i) Not of the expected type, for example executable code rather than user inputted text. ii) Out of range, for example a temperature value which is beyond the limits of a sensor.

Annex D: Modelling approach and key assumptions

A number of key assumptions have been made in carrying out the cost-benefit analysis, due to the lack of available data and evidence on the UK IoT market. These key assumptions are summarised below:

- The growth in the number of consumer IoT devices was forecast using estimates from research carried out by Cambridge Consultants on behalf of Ofcom.[88] These estimates appear to forecast a constant growth of 200,000 devices per year, which DCMS has assumed will continue to 2032.
- It has been assumed that manufacturers will choose to redesign their packaging, rather than use a stick on label. This will result in a one off redesign cost to manufacturers, which it is assumed will not be passed on to UK consumers.
- It has further been assumed that on average, UK IoT manufacturers produce 6 devices, which will each have to be self-certified.
- The estimated number of IoT attacks has been inferred from the proportion of the population that experienced cyber attacks, using data from the Crime Survey for England and Wales,[89] and applied to the forecast for the number of IoT devices. It is further assumed that the level of cyber crime is uniform across the whole of the UK.

[88] Review of the latest developments in the Internet of Things, Cambridge Consultants for Ofcom, 2017.

[89] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

- It is assumed that the proportion of people affected by cyber attacks will remain constant, at a level of 5% of the number of active devices.
- The rate of adoption of secure products has assumed to be on average 15% over 10 years for policy option A.
- It has been further assumed that devices that comply with 3 of the CoP guidelines are on average 40% less likely to be successfully attacked, increasing to 60% less likely when all 13 of the CoP guidelines are followed.

Annex E: Stakeholder views from Secure by Design informal consultation

Informal consultation

Post publication of the March 2018 Secure by Design report, Government launched an informal public consultation, which ran from 7th March 2018 - 25 April 2018, to gather views on the reports proposals and recommendations. An email address was included within the report for people to send feedback to, and the team engaged with a number of stakeholders through roundtables, meetings and formal telephone calls. This amounted to over 70 seperate pieces of feedback.

The main themes of the consultation was that the Code of Practice is a positive collection of best practice within the IoT security world, but that any intervention that sought to fundamentally change industry behaviour would require strong levers (i.e. regulation).

Whilst the feedback was extensive and touched on different aspects of the Government's secure by design work, the following extracts are those which had a focus on regulation:

Feedback from a network security consultant:

"Most of these devices are developed by persons and/or companies with no security knowledge & thus with no regulations to control their actions these persons/companies will continue to deliver shoddily developed software in their products with no consideration given to basic security setup or integration."

Feedback from an internal Cyber Security and Privacy company:

"*Requirements must be put in place for Privacy by Design, including severe penalties for any collecting, storing, and selling (whether directly, or indirectly via use for targeting of advertising) of consumers' personal data if it is not directly required for the correct functioning of the device and service as seen by the consumer.*

No IoT product should even be allowed market access unless it protects consumers' security and privacy. To enforce this, we need regulation, harmonized technical standards and market surveillance authorities with adequate power to remove insecure and privacy endangering products from the market. We strongly believe that the key to improving

security and privacy is to make them mandatory market access requirements. When you have a physical product someone needs to place it in the market. The one who does that must also be responsible for removing it (via a recall) if it is unsafe. Security and privacy must be prerequisites for market access.

Similarly, the requirements should include a strict – and legally enforced - prohibition on any backdoor, including government or law enforcement related, to access user data, usage information, or any form of control over the devices. Additionally, the requirements should include a strict prohibition on vendors providing any such information or control via a "gentlemen's agreement" with a governmental or law enforcement agency/representative.

In terms of the requirements for security and privacy, we believe that any requirements specifically written into law will always be outdated and incomplete. Therefore we believe independent standards agencies should be mandated in a similar way to other internet governing standards bodies. We also recommend that IoT goods are subjected to risk assessments and that these assessments show how any risks have been handled."

Feedback from a leading UK consumer advice organisation:

"As there have already been instances where the security of connected devices has fallen below an acceptable standard, a useful next step would be to consider consumer protections for when things go wrong. It will also be important to ensure that there is clarity around the potential consequences and penalties for companies i.e. might they be required to update/withdraw products from the market and what, if any, communications should be issued to consumers in those circumstances. "

Feedback from a UK based academy of engineering:

"There is also a concern about the effectiveness or timeliness of introducing conventional regulatory measures in the future in response to emerging technological threats. It will take time for international standards to be developed and for a regime that allows compliance to be established, alongside the development of the necessary expertise. In the meantime, several generations of IoT technologies will have been developed, manufactured and distributed around the world. Furthermore, the volumes of components and devices produced make it costly, even if possible, to ensure compliance with security or safety standards and to trace the supply and liability routes back to source.

In order to create a market environment that encourages adherence to standards or codes of practice, or even legislation, responsibilities will need to be placed on UK retailers and distributors through whom IoT products and services will be delivered to consumers. It will then be in their best interests to apply pressure up the supply chain –ultimately to manufacturers, developers and application service providers – to require compliance with the relevant standards and codes of practice. However, this will still not address the distribution of consumer IoT by overseas retailers and distributors. It may be possible to exert some control over consumer IoT connected to mobile networks, but it will be extremely

difficult to enforce any standards on devices connected to consumers' own home Wi-Fi networks. The government should introduce timelines for alternative action, if a voluntary approach is not successful.

Policymakers should consider adaptive methods for governance and regulation, which are built on forward-looking analysis of the benefits and risks of IoT. These methods will help to ensure that regulation keeps up with the fast pace of technological development. Adaptive approaches should draw on continuous cross-domain policy learning by monitoring the adoption and implementation of data protection and cybersecurity guidelines and standards, and by establishing policy reviews and potential sunset clauses.

Many existing regulations are no longer fit for purpose as systems evolve and the threat level changes. Currently, for example, certain manufactured products such as medical devices, toys and electrical products must have a CE mark to demonstrate that they meet safety requirements set out in relevant European Directives. However, safety regulations do not need products to be 'secure by default'. In the future, regulations must integrate safety, security and resilience to protect consumers.

Government will need to review and extend existing safety regulations to take account of cyber safety and resilience. One barrier to creating robust regulations that address the requirements adequately is the lack of sufficient technical expertise within regulators. For example, safety regulators may not have the cybersecurity expertise needed to review safety regulations in the light of security threats and the need for resilience.

Better regulatory impact analysis is required to understand the impact of regulation on innovation and value generation for consumer IoT, and to consider the linkage of regulation. Different regulatory frameworks need to be compatible and useable to ensure that security is adequately addressed. For example, it may be necessary to address the problem of regulatory misalignment between sector-specific regulations and product certification schemes. Regulatory alignment also has an international dimension, given the global supply chains for international products. Government should ensure that robust regulatory impact analysis is carried out.

The separate approaches to regulations and EU directives by different sectors and agencies works against an integrated or systems view of cyber safety and resilience. Where directives are not aligned, there are conflicts that create a barrier to the development of innovations, including poor understanding by companies of directives, delays to innovation and increased costs.

Improvements to legislation that build on existing legislative frameworks around product liability, data protection law and cybercrime will be needed to combat current weaknesses in the law. The complexity of legal agreements underpinning existing IoT products can create unfairness for consumers, because of the difficulty of communicating such complex agreements and because of contradictions in the agreements themselves. Government could consider convening a task force to address how the existing legislative frameworks

can be strengthened, including in the areas of product liability and cybercrime.

Tighter product liability laws that establish accountability for manufacturers of software, hardware and systems should be considered. This would provide an incentive for improving the quality of products. Lowering the evidential barrier for bringing action against the manufacturers of these products would improve consumer protection. Accountability should lie with those who have the power to make changes.

Mandatory updating of devices that contain software and are connected to the internet should be considered. Updates should be made available for the entire operational lifetime of the device. The operational lifetime (period of firmware support) should be defined, with the user encouraged to scrap the device after that period.

As with other types of regulation, the possible impact of tighter product liability laws on smaller companies and on innovation should be considered. The law could protect companies: for example, when software updates are an integral part of a product, the legal terms dictate that if the consumer does not take the updates then the manufacturer is not liable for the non-updated product, although this raises the question of residual liability when support is withdrawn.

Government should monitor the introduction of new data protection legislation in order to learn from implementation challenges and to identify unintended side effects."

Annex F: Glossary of terms

Secure by Design: A design-stage focus on ensuring that security is in-built within consumer IoT products and connected services.

Internet of Things (IoT): The totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

Consumer IoT: This includes consumer purchased 'off the shelf' IoT devices; IoT devices used and installed 'in the home' and the associated services linked to these devices.

Internet connected services: Allowing devices to communicate with other devices over a broad network. These connections usually involve a link occurring between devices and systems and the collection of data.

Distributed Denial of Service (DDoS) attacks: Where many networked devices try to communicate with another at the same time, causing the targeted device to be significantly slower to respond or cease to function.

Botnet: Compromised devices that are grouped together as a network.

Ransomware: Malware that denies access to files or devices until a ransom is paid.

Exploits: Software code or a mechanism that allows unauthorised access to a device.

Device Manufacturer: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.

IoT Service Providers: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.

Mobile Application Developers: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.

Retailers: The sellers of internet-connected products and associated services to consumers.