

Title: Regulation of consumer connectable product cyber security IA No: RPC Reference No: RPC-DCMS-4353(2) Lead department or agency: Department for Digital, Culture, Media and Sport Other departments or agencies: Department for Business, Energy and Industrial Strategy, National Cyber Security Centre	Impact Assessment (IA)
	Date: 21/05/2021
	Stage: Final
	Source of intervention: Domestic
	Type of measure: Primary legislation
	Contact for enquiries: evidence@dcms.gov.uk
Summary: Intervention and Options	RPC Opinion: Fit for purpose

Cost of Preferred (or more likely) Option (In 2019 Prices)			
Total Net Present Social Value	Business Net Present Value	Net cost to business per year	Business Impact Target Status
<i>£6807.5m</i>	<i>£1246.9m</i>	<i>£23.9m</i>	Qualifying Provision

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

Consumer connectable products that have universal default passwords, are not updated against known security flaws, or are otherwise designed without security in mind pose a serious threat to individual privacy and security. These products also pose a wider threat if a malicious actor takes control and uses them to attack others including businesses, government and infrastructure. The government has been working with the tech industry to better secure consumer connectable products for several years, developing a Code of Practice and international standards. Too many insecure consumer connectable products remain on the market and we need to take steps to ensure that in future, consumers can use these products with confidence. Government intervention is necessary in order to address the asymmetric information problem prevalent within the connectable products market and the lack of economic incentive this creates for manufacturers to build security into their devices.

What are the policy objectives and the intended effects?

The policy objective is to reduce the risk to consumers, networks, businesses and infrastructure of the range of possible harms that may arise from vulnerabilities and inadequate security measures in consumer connectable products. In taking action to reduce the risks that these products present, we hope to achieve the following effects:

- Protect consumers, networks, businesses and infrastructure from harm. Insecure connectable products can be used by hostile actors to steal data, seize control of equipment and cause other harms.
- Enable emerging tech to grow and flourish by improving security, and increasing consumer confidence.
- Demonstrate the UK’s continued global leadership in cyber security. The Code of Practice we published in 2018 has been adopted by many countries across the world and has influenced the development of international standards. We will now lead the way to ensure that standards are applied and enforced.

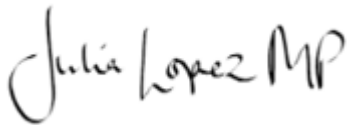
What policy options have been considered, including any alternatives to regulation?

- **Option 0:** Do nothing

- **Option A (non-legislative option):** The Government would introduce a voluntary security label for use by manufacturers of consumer connectable products. This would help consumers to determine whether a product complies with a minimum security baseline that would initially be aligned to the top three Code of Practice guidelines.
- **Option B: (legislative option):** Mandate retailers to only sell consumer connectable products that have a security label indicating whether or not the device meets a minimum security baseline, that would initially be aligned to the top three Code of Practice guidelines (positive label if the security requirements are met and negative if they are not). Manufacturers will be required to self-assess their consumer connectable products.
- **Option C (preferred legislative option):** Legislate to ensure that consumer connectable products made available to UK customers comply with a minimum security baseline, initially aligned to the top three guidelines set out in the Code of Practice for Consumer IoT Security.

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister:



Date: 12th October 2021

Summary: Analysis & Evidence - Policy Option A

Description: The Government would introduce a voluntary security label for use by manufacturers of consumer connectable products. This would help consumers to determine whether a product complies with a minimum security baseline that would initially be aligned to the top three Code of Practice guidelines.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period (Years)	Net Benefit (Present Value (PV)) (£m)		
2019	2020	10	Low (worst): £-28.4m	High (optimistic): £140.1m	Central Estimate: £3.7m

COSTS (£M)		Total Transition (2022)	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£12.0m		Currently un-monetised	£12.0m
High	£29.6m		Currently un-monetised	£29.8m
Central Estimate	£24.4m		Currently un-monetised	£24.6m

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

Transition costs include familiarisation costs associated with implementing the label and these costs impact all retailers and manufacturers within scope. Ongoing costs include self-assessment costs and only affect manufacturers. DCMS estimates that there are 170 manufacturers in scope. In addition to this, DCMS has estimated that there are 3,485 retailers and 11,200 charity stores, which combined make up all retailers within scope.

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

As consumers become more informed through the voluntary label, manufacturers who produce products without a label may incur reputational damage if consumers assume that this signals an insecure device. This could result in lower sales leading to lower profits.

BENEFITS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefits (Present Value)
Low	£0m		£0.2m	£1.4m
High	£0m		£18.6m	£152.2m
Central Estimate	£0m		£3.6m	£28.3m

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 products purchased by consumers, as well as secondary benefits of security improvements in consumer connectable

products. This should result in a reduction in the number of cyber attacks that consumers experience. However, the adoption of the labelling scheme is expected to be low under the voluntary scheme and therefore any benefit to consumers will be more limited.

Other key non-monetised benefits by ‘main affected groups’

Selling products with a 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 without a 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.

Key assumptions/ sensitivities / risks	Discount rate (%)
	3.5%
<ol style="list-style-type: none"> 1. It has been assumed that the adoption of the voluntary label will occur gradually, as manufacturers incorporate the label into their business as usual updates to their packaging to minimise their costs. To this end, it has been assumed that there will be no additional costs associated with adding the voluntary label to packaging. 2. It has been assumed that only those manufacturers that already comply with the security requirements will opt-in to the voluntary labelling scheme. This estimated level of compliance with the security requirements is based on the number of organisations that have publicly announced their commitment to adopt the security requirements set out in the Code of Practice (1.8% as a proportion of manufacturers in the central and optimistic scenario). In the worst case scenario, it has been assumed that only 0.27% of new products are purchased with a positive label throughout the appraisal period, which is based on a sample of 253 Which? Investigations and the probability that a product within that sample met all three security requirements. 3. The proportion of consumers that are predicted to switch to a product with a positive label in the central case scenario is 10% in year 1 of the appraisal period but increases by 1% per year throughout the appraisal period to 19% in year 10. This is based on food labelling research. 4. In the central scenario, it has been assumed that consumers of products that meet the minimum security baseline are 50% less likely to be a victim of cyber crime (relative to a device that does not meet any of the security requirements comprising the minimum security baseline). 5. It has been estimated that businesses account for 18% of all consumer connectable product purchases. 6. The number of specialised stores for the retail sale of electrical household appliances in the United Kingdom (UK) has been used as a proxy for the number of retailers in scope. 	

BUSINESS ASSESSMENT (Option A)

Direct Impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs:	Benefits:	Net:	
£2.9m	£0.0m	£2.9m	£14.3m

Summary: Analysis & Evidence - Policy Option B

Description: Mandate retailers to only sell consumer connectable products that have a security label indicating whether or not the device meets a minimum security baseline, that would initially be aligned to the top three Code of Practice guidelines (positive label if the security requirements are met and negative if they are not). Manufacturers will be required to self-assess their consumer connectable products.

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	PV Base Year 2020	Time Period (Years) 10	Net Benefit (Present Value (PV)) (£m)		
			Low (worst): £-446.3m	High (optimistic): £6435.2m	Central Estimate: £1055.0m

COSTS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£63.3m		£0.8m	£70.3m
High	£507.8m		£2.2m	£526.9m
Central Estimate	£126.8m		£1.8m	£142.5m

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

Transition costs include familiarisation costs; labelling costs as well as costs associated with the disposal of non-compliant products. Labelling costs just affect manufacturers of consumer connectable products, while familiarisation costs and costs associated with the disposal of products impacts both retailers and manufacturers. Ongoing costs include self-assessment costs and only affect manufacturers. DCMS estimates that there are 170 manufacturers in scope. In addition to this, DCMS has estimated that there are 3,485 retailers and 11,200 charity stores, which combined make up all retailers within scope.

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.

BENEFITS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefits (Present Value)
Low	£0		£10.2m	£80.6m
High	£0		£798.3m	£6505.5m
Central Estimate	£0		£153.6m	£1197.5m

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 products purchased by consumers, as well as secondary benefits of security improvements in consumer connectable products. This should result in a reduction in the number of cyber attacks that consumers experience.

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

The sale of consumer connectable products with a 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 cyber attacks. There is also a significant potential benefit to wider society of having fewer insecure consumer connectable products on the market open to hacking and use in wide-scale Distributed Denial of Service (DDoS) attacks.

Key assumptions/ sensitivities / risks

Discount rate (%)

3.5%

1. The proportion of manufacturers that are predicted to adopt the minimum security baselines and therefore have a positive label is assumed to rise gradually over time from 25% in year 1 of the appraisal period to 90% from 2025.
2. The proportion of consumers that are predicted to switch to a product with a positive label in the central scenario is 10% in year 1 of the appraisal period, but increases by 1% per year throughout the appraisal period to 19% in year 10.
3. It has been assumed that retailers will dispose of 10% of their current stock of consumer connectable products in the central estimate (5% in the optimistic scenario and 45% in the worst case scenario).
4. In the central scenario, it has been assumed that consumers of products that meet the minimum security baseline are 50% less likely to be a victim of cyber crime (relative to a device that does not meet any of the security requirements that comprise the minimum security baseline).
5. It has been estimated that businesses account for 18% of all consumer connectable product purchases.
6. The number of specialised stores for the retail sale of electrical household appliances in the United Kingdom (UK) has been used as a proxy for the number of retailers in scope.

BUSINESS ASSESSMENT (Option B)

Direct Impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs: £15.8m	Benefits: £0.0m	Net: £15.8m	£79.1m

Summary: Analysis & Evidence - Policy Option C

Description: Legislate to mandate a minimum security baseline for consumer connectable products, with this baseline initially aligning to the top three guidelines of the Code of Practice.

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	PV Base Year 2020	Time Period (Years) 10	Net Benefit (Present Value (PV)) (£m)		
			Low (worst): £379.4m	High (optimistic): £16431.5m	Central Estimate: £6807.5m

COSTS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£85.0m		£2.0	£102.6
High	£553.6m		£5.3	£599.3m
Central Estimate	£170.0m		£4.9	£212.m

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

Transitional costs include familiarisation costs, costs associated with implementing a statement of compliance, as well as costs associated with the disposal of non-compliant products. The transitional costs identified here are likely to affect both manufacturers and retailers. Ongoing costs include self-assessment costs as well as costs associated with implementing the three security requirements that comprise the initial minimum security baseline, and these costs only affect manufacturers. DCMS estimates that there are 170 manufacturers in scope. In addition to this, DCMS has estimated that there are 3,485 retailers and 11,200 charity stores, which combined make up all retailers within scope.

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

It has not been possible to capture all indirect costs that may result from the introduction of this legislation. For instance, it is possible that certain products will no longer be available on the UK market due to non-compliance, which could result in less choice for consumers and a potential loss of revenue for businesses.

BENEFITS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefits (Present Value)
Low	£0		£119.9m	£978.7m
High	£0		2022.4m	£16534.0m
Central Estimate	£0		£868.0m	£7019.5m

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

It is expected that the main benefits of this policy option will accrue from a reduction in the number of insecure consumer connectable products purchased by customers, as well as secondary benefits of security improvements in consumer connectable products. This should result in a reduction in the number of cyber attacks that customers experience.

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

The direct benefits to consumers from a reduction in the number of cyber crime incidents has been estimated, however, the benefits to wider society from a reduction in cyber crime has not been captured.

Key assumptions/ sensitivities / risks

Discount rate (%)

3.5%

1. It has been assumed that retailers will dispose of non-compliant stock resulting in a loss of revenue. The central estimate is that 10% of stock will be disposed of, which is based on the proportion of devices with default passwords (according to 253 Which? investigations). The optimistic estimate is that 5% of products will be disposed of and in the worst case scenario 45% of products will be disposed of.
2. All 'small' manufacturers pass their direct costs onto consumers. Using IoTUK data, it has been estimated that 72% of manufacturers are 'small' and 98% of retailers are either 'small' or 'micro' businesses.
3. In the central scenario, it has been assumed that mandating the initial minimum security baseline leads to a 50% reduction in the number of cyber crime incidents.
4. It has been estimated that businesses account for 18% of all consumer connectable product purchases.
5. The number of specialised stores for the retail sale of electrical household appliances in the United Kingdom (UK) has been used as a proxy for the number of retailers in scope.

BUSINESS ASSESSMENT (Option C)

Direct Impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs: £23.9m	Benefits: £0.0m	Net: £23.9m	£119.5

Table of Contents

Summary - Intervention and Options	1
Summary - Analysis & Evidence - Policy Option A	3
Summary - Analysis & Evidence - Policy Option B	5
Summary - Analysis & Evidence - Policy Option C	7
Section 1 - Products in scope	12
Section 2 - Problem under consideration	13
2A - Growth of consumer connectable products	13
2B - The Impact of COVID-19 on consumer connectable products	13
2C - Security vulnerabilities in consumer connectable products	14
2D - Impact of insecure consumer connectable products on citizens	14
2E - Botnets and the impact of insecure consumer connectable products on networks and infrastructure	16
2F - Impact of insecure consumer connectable products on businesses	18
2G - Summary of the risks of insecure consumer connectable products	19
2H - Previous UK Government Interventions	19
2I - Prevalence of baseline security measures	21
<i>2I(i) - Progress in eliminating Universal Default Passwords</i>	22
<i>2I(ii) - Prevalence of Vulnerability Disclosure Policies</i>	22
<i>2I(iii) - Prevalence of timely software updates, and transparency on how long products will receive security updates for</i>	23
2J - What sectors / markets / stakeholders will be affected, and how, if the government does intervene?	23
Section 3 - Rationale for intervention	24
3A - Externalities	24

3B - Information Asymmetry	24
3C - Misaligned Incentives	25
3D - Summary of Market Failures	25
Section 4 - Policy objective	26
Section 5 - Description of preferred option and plan for implementation	27
5A - Shortlisted policy interventions	27
<i>5A(i) - Option 0 - Do Nothing (counterfactual)</i>	27
<i>5A(ii) - Option A - Voluntary Security Labelling Scheme</i>	28
<i>5A(iii) - Option B - Mandatory Security Labelling Scheme</i>	28
<i>5A(iv) - Option C - Legislating to mandate a minimum security baseline for consumer connectable products</i>	28
5B - Description of preferred option	29
5C - How the preferred option will be given effect	33
5D - How the intervention would meet our policy objectives	33
5E - When will the arrangements come into effect	34
Section 6 - Proportionality approach	35
6A - Extent of analysis and further impact assessment publications	35
6B - Proportionate analytical approach for indicative cost-benefit analysis	37
Section 7 - Indicative Cost-Benefit Analysis	38
7A - Structure of the Indicative Cost-Benefit Analysis	40
7B - Underlying methodology common to all options	41
<i>7B(i) - Estimating the number of consumer connectable products</i>	41
<i>7B(ii) - Estimating the replacement rate of consumer connectable products</i>	43
<i>7B(iii) - Estimating the cost of cyber attacks</i>	46

7C - Benefits methodology of relevance to all options	48
<i>7C(i) - Estimating the benefits resulting from reduced cyber crime</i>	48
<i>7C(ii) - Non-monetised benefits</i>	57
7D - Costs methodology of relevance to all options	58
<i>7D(i) - Estimating the number of manufacturers and retailers of consumer connectable products</i>	58
<i>7D(ii) - Estimating familiarisation costs</i>	58
<i>7D(iii) - Estimating self-assessment costs</i>	61
<i>7D(iv) - Estimating costs to retailers</i>	62
7E - Cost methodology not of relevance to all options	63
<i>7E(i) - Estimating the cost of labelling</i>	63
<i>7E(ii) - Estimating the cost of implementing security improvements</i>	65
<i>7E(iii) - Estimating the cost of publishing and verifying a statement of compliance</i>	68
<i>7E(iv) - Estimating the costs associated with the disposal of non-compliant goods</i>	69
<i>7E(v) - Estimating the costs of enforcement</i>	71
Section 8 - Additional Analysis	74
8A - Analysis of the potential costs to consumers	74
<i>8A(i) - Policy Option B - Mandatory security labelling scheme</i>	74
<i>8A(ii) - Policy Option C - Mandatory security baseline</i>	74
8B - Analysis of the impact on small and micro businesses	76
8C - Break-Even Analysis	80
8D - Analysis of potential trade impacts	81
<i>8D(i) - Policy Option B - Mandatory security labelling scheme</i>	81
<i>8D(ii) - Policy Option C - Mandatory security baseline</i>	82
8E - Equalities Impact Assessment	82
8F - Assessment of impact on innovation	83

Section 9 - Monitoring and evaluation	84	
9A - Evaluation of objectives	84	
9B - Proportionality of monitoring and evaluation considerations in this and future impact assessment publications	84	
9C - Indicative monitoring and evaluation considerations	85	
Annex 1 - Top three consumer connectable product security guidelines	87	
Annex 2 - Description of the policy development process, and other policy options considered	89	
Annex 3 - Risks and Assumptions	101	

Section 1 - Products in scope and key terminology

1. The PSTI Bill product security measures will apply to a broad range of consumer network-connectable products. This includes smartphones, as well as products that are primarily used by consumers but can also be used in a business environment. The non-exhaustive list in [Box 1](#) contains examples of products included within the scope of the regulation. Further details of the way in which the PSTI Bill product security measures will define products included within scope are provided in the subsequent section - [5B - Description of preferred option](#).

Box 1 - Non-exhaustive list of products within the scope of the intended regulation

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

2. Some aspects of the mandatory minimum security baseline in the Government’s intended intervention will apply only to network-connectable devices made available primarily to consumers. Other aspects will apply to both these devices, and any digital services associated with the device, such as mobile applications and cloud storage. The term ‘**products**’ should be understood to refer to both ‘**devices**’ and their ‘**associated services**’.
3. The term ‘**consumer connectable products**’ will be used throughout the impact assessment to refer to all products included within the scope of the PSTI product security measures, or would otherwise fall within scope, but are likely to be explicitly excepted when the legislation comes into force.
4. Outside of this impact assessment, the terms ‘**internet of things (IoT)**’ or ‘**smart technology**’ can have various connotations. It is sometimes used in a way that is largely interchangeable with ‘consumer connectable products’, but can also variably be understood to refer to internet-connectable products only, consumer products as well as products intended primarily for industrial use, or physical devices exclusively without their associated services. These terms have been included in this impact assessment in instances where it was used in externally cited reports, or as part of previous Government publications.
5. Definitions of these key terms for the purposes of this impact assessment are detailed in [Box 2](#):

Box 2 - Key impact assessment scope terminology

Device	<i>Physical thing, including its hardware and software components</i>
Associated Services	<i>Digital services that, together with the device, are part of the overall product and that are required to provide the product’s intended functionality.</i>
Product	<i>‘device’ and its ‘associated services’</i>

Section 2 - Problem under consideration

6. Whilst the growing adoption of an increasingly diverse range of consumer connectable products offers a wealth of benefits to UK consumers and businesses, progress has not been fast enough in addressing basic security vulnerabilities in these products, resulting in citizens, networks and the wider economy being unnecessarily exposed to a range of harms.

2A - Growth of consumer connectable products

7. Ofcom estimates that in 2016 there were 13.3 million IoT connections in the UK, of which 5.7 million were consumer electronics and fast moving consumer goods, such as consumer wearables, household electricals and smart home devices. By 2024, this is estimated to increase to 39.9 million connections.¹ In addition to this, there were an estimated 58 million smartphone users in the UK in 2019. This is expected to increase to 61 million by 2024.²
8. A 2020 survey of 3,959 consumers by Ofcom found that the most prevalent internet-connectable devices in the UK include:³
 - **Smartphones** – used by 82% of respondents
 - **Smart TVs** – 98% had a TV set, 58% of those participants said it was a TV that connected to the internet
 - **Wearable devices** – in 18% of households, including fitness trackers that monitor physical activity and location
 - **Smart speakers** – in 22% of households, which can react to voice commands and be used to control other devices
9. The adoption of consumer connectable products is only expected to grow in the future, as advancements in technology such as 5G will reduce the latency of device communications, improving user experience. Moreover, as the cost of integrating internet connectivity to devices falls, manufacturers will continue to connect more and more devices to the internet.⁴
10. The integration of connectivity will also help to improve functionality within more products, benefiting both manufacturers and technological innovators through creating products that better reflect how consumers use the devices.⁵

2B - The Impact of COVID-19 on consumer connectable products

11. The overall impact of COVID-19 on consumer connectable products within the UK is not yet clear, However, there is evidence to suggest that the COVID-19 pandemic has resulted in higher consumption of consumer connectable products, likely driven by the increase in remote working. For example, since the COVID-19 pandemic in March 2020, six in ten consumers in the UK (57%) report an increase in their household use of smart devices.⁶ Furthermore, according to the Vodafone IoT spotlight Report 84% of businesses claimed IoT was essential for their survival during the COVID-19 pandemic⁷.
12. There is also evidence that cyber attacks have increased during the pandemic. According to research undertaken by Checkpoint, “71% of security professionals have noticed an increase in security threats or attacks since the beginning of the pandemic”⁸. To this end, there is evidence to suggest that the pandemic has left consumers more dependent on consumer connectable products and without the necessary security measures in place has also left them vulnerable to cyber attacks. Therefore, with evidence suggesting an

¹ [Review of the latest developments in the Internet of Things. Ofcom, 2017](#)

² S. O’Dea, 2020, Forecast of smartphone user numbers in the United Kingdom (UK) 2018-2024
<https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/>

³ Ofcom, 2020. [Technology Tracker 2020 Data Tables](#)

⁴ CSES, 2020. [Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things \(IoT\) Landscape.](#)

⁵ CSES, 2020. [Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things \(IoT\) Landscape.](#)

⁶ Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

⁷ Vodafone IoT Spotlight Report, 2020 - <https://www.vodafone.com/business/news-and-insights/white-paper/iot-spotlight-2020>

⁸ <https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/>

increase in (i) demand for consumer connectable products and (ii) an increase in security threats there is a growing need for more secure products in order to protect consumers.

2C - Security vulnerabilities in consumer connectable products

13. Consumer connectable products are becoming increasingly prevalent in people's everyday lives, but large numbers of these products are sold to consumers without even basic cyber security provisions, for example a vulnerability disclosure policy which allows security researchers to report vulnerabilities to the manufacturer.⁹
14. Consumers are both unaware that their connectable products are potentially insecure¹⁰, whilst also not being provided with sufficient information about the security of these products to allow them to make an informed purchasing decision.¹¹ Moreover, only one in five consumers are actively taking steps to check the security provisions linked to their connectable products.¹²
15. The characteristics of consumer connectable products are one factor that contributes to a lack of security being built in by design. Physical devices are often designed with a focus on user convenience (e.g. small or low-powered), but this can be at the expense of other functionality including security. This can limit a device's capability for basic security features, such as encryption.
16. Furthermore, the user interface of many consumer connectable products, such as screens or keypads, is often omitted from the device itself, as it may affect a device's functionality. The lack of user interface makes it harder for consumers to change default passwords, change security settings and update their device, making them less secure.¹³¹⁴

2D - Impact of insecure consumer connectable products on citizens

17. Insecure consumer connectable products can lead to people's privacy and safety being undermined, as these vulnerable products are normally connected to people's home networks. If just one connectable product in a consumer's home network lacks basic cyber security measures, this could allow a cyber criminal to easily gain access to the entire home network.
18. When security flaws in products connected to the home network are exploited, compromised services can pose a significant risk to consumers' other connectable products and their wider network. 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 or harass them. Some connectable products designed for children have had security issues that left voice recordings and imagery (that families believed were private) open to the public, or easily accessible to hackers.
19. A compromised product 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. In 2016 the heating in two apartment buildings in Finland was disrupted for almost a week after the system suffered a distributed denial-of-service (DDoS) attack. The problem was only resolved once the building heating systems were manually disconnected from the internet.¹⁵ A DDoS attack is defined by the NCSC as when legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. This can include a botnet which is a network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.¹⁶

⁹ IoTSEF, 2020. Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report.

<https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSEF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf>

¹⁰ Harris Interactive, February 2019. Consumer Internet of Things Security Labelling Survey Research Findings Report.

¹¹ Blythe, J.M., Sombatruang, N., Johnson, S., 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?

¹² Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

¹³ McFadden, M., Wood, S., Magtani, R., Forsyth, G., 2019. The economics of the security of consumer-grade IoT products and services. [https://www.internetsociety.org/wp-content/uploads/2019/04/The Economics of Consumer IoT Security.pdf](https://www.internetsociety.org/wp-content/uploads/2019/04/The_Economics_of_Consumer_IoT_Security.pdf)

¹⁴ Default passwords are passwords that are preinstalled on a device, and would be set to the same configuration value following a factory reset. Default passwords that are universal or easily guessable or derivable can weaken security

¹⁵ International Business Times, 2016, accessed at:

<https://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639>

¹⁶ NCSC Glossary: <https://www.ncsc.gov.uk/information/ncsc-glossary>

20. Alternatively, if smart locks or connectable physical access control systems are compromised, criminals could get into homes without needing to force entry.¹⁷ In 2019, F-Secure consultants found a vulnerability in a smart lock that allowed hackers to pick the lock. However, as the manufacturer was unable to update the device, this left users vulnerable to attacks unless they physically uninstalled and replaced their door lock.¹⁸ This poses both a safety and security risk to homeowners.
21. Consumer connectable products also have the potential to cause physical harm to their users. University College London conducted a systematic review to identify risks from the consumer Internet of Things. The study identified a number of high-level mechanisms through which offenders may exploit connectable products including profiling, physical access control and the control of device audio/visual outputs. The types of crimes identified that could be facilitated by the internet of things were wide-ranging and included burglary, stalking, and sex crimes through to state-level crimes including political subjugation.¹⁹ Furthermore, research conducted by consumer group Which? and security consultants NCC Group in 2020 found that some smart plugs on the market contained vulnerabilities that could potentially lead to a fire.²⁰ Of the ten smart plugs that were tested, they found thirteen vulnerabilities in nine of the products, three of which were deemed to be high risk and three critical vulnerabilities. Several devices could allow hackers to steal the network's password which could then be used to hack into other connectable devices.
22. If a vulnerability in a product is not remediated by a manufacturer it can also lead to continued risks to users (see the case study in [Box 3](#) below):

Box 3 - Case Study

In 2017 and 2018, a range of vulnerabilities were identified in smart watches aimed at children. These vulnerabilities were discovered by organisations including the Norwegian Consumer Council and Pen Test Partners.^{21,22} In the case of the research by Pen Test Partners, a vulnerability was identified in the web service that a specific brand of smart watch connected to. This vulnerability allowed an attacker to access personally identifiable information including the linked mobile number and GPS coordinates for the watch. Unfortunately, Pen Test Partners were unable to contact the manufacturer to report the vulnerability – and through further research identified similar vulnerabilities in other models likely produced by a single manufacturer, often called an ODM (Original Device Manufacturer) or an OEM (Original Equipment Manufacturer). The total number of users of these smart watches was determined to be around 1 million globally.

Other product categories where similar issues have occurred include smart home cameras, and Android smartphones.²³ With these, consumers were not given clarity around how long the products would be supported for – leading to vulnerable devices seeing continued use. In all these cases, the PSTI product security framework would have ensured that the manufacturers provide a route for vulnerabilities to be disclosed to them, and that the consumer would have clarity over whether products were still supported.

23. Furthermore, since the COVID-19 pandemic in March 2020, six in ten consumers in the UK (57%) report an increase in their household use of smart devices.²⁴ This increasing reliance on connectable products will have a long term impact because of their use within a work context. Vulnerable consumer connectable products could leave business data at risk. For example, with more organisations moving towards Bring Your Own Device (BYOD) to allow employees to work from home, it is important that consumers and their employers know that products they use for work will receive security updates.

¹⁷ 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/>

¹⁸ <https://www.techradar.com/uk/news/smart-lock-security-issues-leave-the-door-open-for-hackers>

¹⁹ UCL, Blythe J. M. and Johnson S.D, 'A systematic review of crime facilitated by the consumer Internet of Things', Security Journal, 2019.

²⁰ Which?, 2020. [Which? exposes the smart plugs that are open to hackers and could start a fire.](#)

²¹ <https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/>

²² <https://www.pentestpartners.com/security-blog/tracking-and-snooping-on-a-million-kids/>

²³ <https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/> and <https://www.bbc.co.uk/news/technology-51751950>

²⁴ Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

2E - Botnets, and the impact of insecure consumer connectable products on networks and infrastructure

24. As the uptake of consumer connectable products continues to grow, there is an emerging risk that large numbers of these products could be used as part of a coordinated DDoS attack in the future, or have already been used in such an attack. Attacks enabled by botnets (a network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge²⁵) could affect essential systems such as electricity supplies and power grids.²⁶

Box 4 - Case Study

The Mirai Botnet

In 2016, a security researcher identified a new piece of malware that was targeting consumer connectable products such as routers, and video cameras.²⁷ This malware was named Mirai, as that was the name of the malicious file downloaded to compromised devices. The original Mirai malware functions by scanning IP addresses randomly to look for open telnet ports (telnet is an unencrypted protocol used to communicate and interface with a remote device).

Many consumer connectable products that still have open telnet ports have default usernames and passwords (such as "admin"). The Mirai malware would try to log in to these devices over telnet using a list of common username and password combinations. If it could successfully log in, it downloads the Mirai malware to the new device and the process is repeated. Once a device was compromised, it connected to a Command and Control server (a C2 server) which would then be able to give the device instructions. This collective of compromised devices that can be controlled via a C2 server is referred to as a botnet.

In October 2016, a Mirai botnet was used to launch a DDoS attack on the DNS provider Dyn.²⁸ Post-incident analysis by Dyn²⁹ determined that around 100,000 devices were used in this attack – leading to multiple websites including Twitter, Reddit, PayPal, Amazon, Netflix and Spotify going offline.³⁰ Since then, Mirai botnets have been used to attack Liberian internet exchanges³¹, and UK banks including Lloyds and RBS³² leading to disruption to customers.

In addition, many variants of Mirai have appeared – this has been accelerated by the public release of the Mirai source code. However, it has also been enabled by vulnerabilities in consumer connectable products not receiving fixes from manufacturers. For example, earlier in 2020, a Mirai variant was categorised by TrendMicro that exploited nine vulnerabilities including one that was discovered in 2013.³³ It is difficult to precisely identify how many devices are currently in botnets that were created using the Mirai malware. However, data from the security research company GreyNoise shows that it has seen approximately 4.5 million cases where Mirai activity has come from an IP address³⁴, with over 40 thousand based in the UK³⁵ – an indication of a compromised device. This is many times more devices than were used in the attack that successfully disrupted access to commonly used web services and banking websites.

25. Researchers at the University of California sought to determine the cost to consumers of insecure Internet of Things devices³⁶ by examining the impact of three different types of DDoS attacks. Two real life attacks and one hypothetical attack were used as part of this research. Based on electricity and bandwidth consumption of the compromised devices used in the attacks, the researchers estimated the costs that would

²⁵ NCSC Glossary: <https://www.ncsc.gov.uk/information/ncsc-glossary>

²⁶ BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid, Usenix, 2018
<https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf>

²⁷ <https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html>

²⁸ <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

²⁹ <https://web.archive.org/web/20161107182254/http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

³⁰ <https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/>

³¹ <https://grahamcluley.com/did-mirai-botnet-liberia-offline/>

³² <https://www.bbc.co.uk/news/business-38715909>

³³ <https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173/>

³⁴ <https://viz.greynoise.io/query/?qnl=tags%3A%22Mirai%22>

³⁵ <https://viz.greynoise.io/query/?qnl=tags%3A%22Mirai%22%20country%3A%22United%20Kingdom%22>

³⁶ <https://groups.ischool.berkeley.edu/riot/>

be incurred by the owners of devices taken control of by hackers when used in these attack scenarios.³⁷ Information on the limitations of this study are noted below.

26. The University of California's research, which was conducted between 2017 - 2018, focused on malware which can exploit consumer connectable products with default credentials. This vulnerability could be addressed if these devices did not feature universal, easily guessable, or easily derivable default passwords, which would be required by the PSTI product security framework and was also advocated by guideline one of the UK Government's Code of Practice for IoT Security (see [2G - Previous UK Government Interventions](#) for further details).
- The first real life scenario they examined, the Krebs on Security Attack, was a botnet attack against a security researcher's (Krebs) website, launched with the aim of taking the website offline. The attack attempted to flood the website with internet traffic directed from exploited consumer connectable products which had default passwords, allowing the hacker to take control of these devices and use them to target the server that hosted the website. Analysis of the attack suggested that it involved devices from around the world.
 - The second scenario that the researchers modelled was based on the Mirai attack against domain name server provider Dyn (see [Box 5](#)), which took websites including Amazon and Twitter offline for a day.
 - Lastly, they estimated the cost of electricity and bandwidth consumption resulting from a hypothetical attack, using the peak power of Mirai as an example, for an extended period.

Box 5 - Estimated impact of DDoS attacks (University of California)

Attack	Cost
<p>Scenario 1: Krebs On Security Attack³⁸</p> <p>In 2016, the Mirai and BASHLITE botnets were targeted against the cyber security blog KrebsOnSecurity.com in a DDoS attack. This brought the site down following an attack size of approximately 620 Gbit/s. This remains one of the largest botnet-enabled DDoS attacks. Both the Mirai and BASHLITE botnets were constructed of compromised connected devices which had default passwords.</p>	<p>According to their cost calculator, the total electricity and bandwidth consumption costs borne by consumers in this attack was \$323,973.75.</p>
<p>Scenario 2: The Dyn, Inc. Attack</p> <p>Dyn, a US DNS (Domain Name System) hosting service, was a victim of a botnet-enabled DDoS attack. This took down a number of essential services, including several American banks, Twitter etc. The attack occurred because malware took control of roughly 600,000 vulnerable connected devices, particularly smart security cameras, which had default passwords.³⁹ This incident could easily be replicated and with worse effect (such as a long-lasting DDoS attack on UK banking and government services) due to new products being made available with universal, easily guessable, or easily derivable default passwords.</p>	<p>Total electricity and bandwidth consumption costs borne by consumers as \$115,307.91.</p>
<p>Scenario 3: "Worst-Case" Attack.</p> <p>This hypothetical "Worst-Case" scenario approximates the costs that could result if the Mirai botnet operated at its peak power.</p>	<p>The projected total electricity and bandwidth consumption costs to consumers of this attack is \$68,146,558.13.</p>

³⁷ Definition of device bandwidth: the amount of data that can be transmitted in a fixed amount of time. It should be noted that these costs only capture electricity and bandwidth costs and do not capture all costs associated with such an attack.

³⁸ <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>

³⁹ <https://www.wired.com/story/mirai-botnet-minecraft-scram-brought-down-the-internet/>

27. Research by BitSight found that around 8% of web domains which relied on Dyn's services stopped using their services after the attack.⁴⁰ This demonstrates that cyber security can have a real commercial impact on businesses.
28. While the University of California study provides an estimate of the cost of electricity and bandwidth consumption, it does not consider the wider harms as a result of their devices being used in a wide scale DDoS attack. This could include, for example, emotional distress of victims, loss of essential services, attacks on critical national infrastructure such as the use of high wattage domestic appliances to launch large-scale coordinated attacks on power grids, and financial losses for businesses affected. Further information on this can be found in the section of this Impact Assessment detailing our benefits calculation methodology ([7C - Benefits methodology of relevance to all options](#)), and in [NCSC Statement 6](#).
29. It is important to note that criminals or nation states have also been able to create botnets spanning huge geographical locations (such as Mirai, VPNFilter, Satori, etc), through the use of unpatched vulnerabilities in consumer connectable products. These have been used to target critical infrastructure in a country, such as the attacks on Lloyds Bank, and Barclay's in the UK and the attacks that caused disruption to internet access in Liberia.

2F - Impact of insecure consumer connectable products on businesses

30. It is not only individuals that use consumer connectable products. Businesses and their employees also bring these products into their operations, connecting them to their network and therefore exposing their businesses to the risks posed by insecurities in these products. In a survey undertaken by the 'Centre for Strategy and Evaluation Services' in 2020, 28% of businesses reported using consumer IoT devices.⁴¹
31. A 2018 survey predicted that IoT would become important for 92% of businesses in 2020.⁴² 50% of 950 companies surveyed globally in 2018 reported using IoT devices made by a third party, and 33% used their own IoT devices.⁴³ However only 42% of UK respondents reported that their organisations were able to detect when any of their IoT devices had been breached.⁴⁴
32. Moreover, research in 2019 found that 49% of UK businesses had unknown devices on their network.⁴⁵ This creates a risk which could be exploited if devices on a business network do not have basic cyber security controls, potentially leading to widespread disruption within an organisation as well as costs associated with reputational and physical damage, decreased productivity and loss of business. This was demonstrated by the VPNFilter malware, which infected over 500,000 consumer and small-business grade devices globally in 2018.⁴⁶
33. Additionally, statistics from 2018 highlight that in the UK, 45% of businesses allowed staff to use personally-owned devices for regular work.⁴⁷ This figure illustrates the increasing dependence that businesses are placing on connected devices as part of ensuring workers are able to operate effectively. It also raises the concern that as consumer connectable products are increasingly used within businesses, the challenges of assessing the risks and preventing vulnerable products from accessing their networks rises significantly.
34. A 2020 report by information security company Zscaler, analysing 500 million transactions from more than 2000 of its enterprise consumers, found that employees are frequently connecting their personal devices to the enterprise network, and that only 17% of IoT-based transactions are using secure connection protocols, with the remaining 83% of IoT-based transactions using plain text channels, exposing this traffic to a range of exploits.
35. The 2020 Cyber Security Breaches Survey found that the average cost of a breach with an outcome was £3,230. For medium and large firms, the average cost was £5,220.⁴⁸ Although the breaches in this survey

⁴⁰ <https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/>

⁴¹ 36 organisations provided a response to the survey question 'What is your organisation's relationship with consumer Internet of Things (IoT) devices?'

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900327/Framing_the_nature_and_scale_of_cyber_security_vulnerabilities_within_the_current_consumer_internet_of_things_iot_landscape.pdf page 63.

⁴² State of IoT security survey 2018, Digicert. Survey of 700 organisations across UK, France, Germany, US, Japan.

<https://www.digicert.com/resources/state-of-iot-security-report-survey-2018.pdf>

⁴³ Gemalto, 2018. State of IoT Security Report. <https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf>

⁴⁴ Gemalto, 2018. State of IoT Security Report. <https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf>

⁴⁵ <https://www.information-age.com/uk-businesses-iot-ot-cyber-attacks-123479373/>

⁴⁶ <https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/>

⁴⁷ Statista. 2020. Share of United Kingdom (UK) business where bringing your own device occurs in 2018

⁴⁸ Cyber Security Breaches Survey 2020.

may not have been caused by insecure consumer connectable products, this demonstrates that cyber attacks against organisations can potentially have a significant financial impact.

Box 6 - Case Study

Casino cyber attack in 2017

In 2017, a casino in North America experienced a cyber attack which involved the loss of vast amounts of business data (10GB) due to a vulnerability found within a connected fish tank. The fish tank had sensors connected to a computer that regulated the temperature, food and cleanliness of the tank. The smart thermometer in the fish tank had a vulnerability which was exploited by the hackers to access the casino's wider network. Limited information has been provided about the particular vulnerability and the types of data that were stolen.

However, this case study is important because it highlights how a seemingly insignificant decision to install an aquarium with a vulnerable connectable product into a casino provided hackers with the means to breach that organisation's network.⁴⁹

2G - Summary of the risks of insecure consumer connectable products

36. The risk to consumers and the wider economy from insecure consumer connectable products is a function of both the impact of these vulnerabilities and the likelihood of them being exploited. Both the likelihood and impact are also influenced by the threat landscape. As cyber criminals become more sophisticated, the threat will continue to evolve.
37. Examples of cyber attacks using consumer connectable products, against individuals and the wider economy, have shown that impacts can be significant at both a personal and economic level. Moreover, as consumer connectable products are adopted more widely, the opportunity for criminals to take advantage of these vulnerabilities increases, increasing the likelihood of cyber crime enabled by insecure consumer connectable products.
38. Therefore, the risk to the UK economy and society as a result of these products will only increase in the future. Consumers also have a limited ability to mitigate these risks. A study suggests there are up to forty-three behaviours expected of consumers to protect consumer connectable products across their lifecycle.⁵⁰ Moreover, consumers lacking technical knowledge, devices coming with poorly-designed or non-existent user interfaces, and the increasing market share of cheap connectable products relative to non-connected alternatives, all compound these risks further.

2H - Previous UK Government Interventions

39. On the 1st November 2016, the UK Government published a National Cyber Security Strategy, setting out the government's plans to make Britain secure and resilient in cyberspace. As part of this strategy, the government detailed an objective to ensure that "the majority of online products and services coming into use become 'secure by default' by 2021".⁵¹ (See [Box 7](#) for further details)

⁴⁹ Washington Post, 'How a fish tank helped hack a casino', 21 July 2017,

<https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/>

⁵⁰ Blythe, J. M., Michie, S., Watson, J., & Lefevre, C. E. (2017). Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours. *Frontiers in Public Health*. <https://doi.org/10.3389/conf.FPUBH.2017.03.00021>

⁵¹

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Box 7 - National Cyber Security Strategy (2016 - 2021)

Strategic Objective 5.2.3

“The majority of online products and services coming into use become ‘secure by default’ by 2021. Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected.”

40. From December 2016 to February 2018, the UK Government conducted a review to identify proposals for improving the cyber security of consumer IoT devices and associated services. As part of this review, the UK Government set up an Expert Advisory Group and engaged with over 100 stakeholders including industry, academics, retailers, consumer associations and international governments.
41. On the 7th of March 2018, the UK Government published the Secure by Design report, which called for a fundamental shift in industry’s approach to managing cyber risks, advocating for a move away from placing the burden on consumers to securely configure their devices, and instead ensuring that strong security is built in by design.⁵² This report was developed through extensive engagement with industry and subject matter experts.
42. The Government’s preference has always been for the market to be able to solve the problems presented by insecure consumer connectable products, and to this end, a central component of the Secure By Design report was a draft Code of Practice aimed primarily at manufacturers of consumer IoT products, which set out thirteen outcome-led guidelines that manufacturers would need to implement in order to improve the cyber security of their consumer IoT products.
43. This draft report was subject to an informal consultation from the 7th of March to the 25th of April 2018, and additional feedback from NCSC, industry, academic institutions and civil society helped shape a finalised Code of Practice for Consumer IoT Security, which was published on the 14th of October 2018.⁵³ The thirteen outcome-led guidelines featured in the Code of Practice are detailed in [Box 8](#).
44. The Code of Practice recommended that three guidelines in particular (henceforth referred to as the “top three”) should be implemented as a priority, as doing so would bring the largest security benefits in the short term. [NCSC Statement 1](#) provides further details of the importance of implementing the top three Code of Practice guidelines.

Box 8 - Code of Practice for Consumer IoT Security guidelines

Top three guidelines

No default passwords - All IoT device passwords shall be unique and not resettable to any universal factory default value.

Implement a vulnerability disclosure policy - All companies that provide internet-connected devices and services 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. Disclosed vulnerabilities should be acted on in a timely manner.

Keep software updated - Software components in internet-connected devices should be securely updatable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reason for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.

Additional guidelines

⁵² <https://www.gov.uk/government/publications/secure-by-design-report>

⁵³

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Securely store credentials and security-sensitive data
Communicate securely
Minimise exposed attack surfaces
Ensure software integrity
Ensure that personal data is protected
Make systems resilient to outages
Monitor system telemetry data
Make it easy for consumers to delete personal data
Make installation and maintenance of devices easy
Validate input data

NCSC Statement 1

Impact of the top three Code of Practice guidelines

“The NCSC’s view is that the top three principles within the Code of Practice and ETSI EN 303 645 will make the most fundamental difference to the vulnerability of consumer connectable products in the UK, are proportionate given the threats, and universally applicable to devices within scope. While the other requirements in the Code of Practice and EN 303 645 could reduce the potential vulnerabilities that may be discovered in a device, if those vulnerabilities can’t be easily reported, and users don’t know if their device can still receive updates then devices will remain at high risk. In this situation, the other requirements would make minimal difference.”

45. Additional details of the security issues underpinning the top three Code of Practice guidelines can be found in [Annex 1 - Top three consumer connectable product security guidelines](#).
46. DCMS and NCSC also worked with industry and collaborated closely with the European Telecommunications Standards Institute (ETSI), a standards development organisation that develops globally-applicable standards, to develop an international standard, ETSI EN 303 645, setting our security provisions for smart devices. The standard was published in June 2020 and expanded on the Technical Specification published by ETSI in February 2019 by providing more guidance and a better framework to enable assessment of products.
47. Further details of the policy development process undertaken to identify the most appropriate government intervention to address the issue of insecure consumer connectable products can be found in [Annex 2 - Description of the policy development process, and other policy options considered](#).

21 - Prevalence of baseline security measures

48. Evidence suggests that the level of security in consumer connectable products has not significantly improved in recent years, despite the publication of guidelines for improving the cyber security of these products in the Code of Practice for Consumer IoT Security.⁵⁴ Only three manufacturers of consumer connectable products have publicly pledged to the Code since it was first launched⁵⁵. It is not anticipated that the level of voluntary adoption will significantly increase in the future, due to the current lack of incentives for manufacturers to embed security into their devices (see [Section 3 - Rationale for intervention](#) for further details).
49. The following sections detail available evidence on the extent to which consumer connectable products being made available to UK consumers comply with the top three guidelines (See [Annex 1 - Top three consumer connectable product security guidelines](#) for further details of the security issues that informed these guidelines). It may be the case that many more products lacking basic security measures are in use that this evidence implies, as although some manufacturers may no longer produce devices with default passwords for example, older versions of these devices may still be actively used by owners. These are known as legacy products. Despite being insecure, these legacy products may remain connected to the network, even after updated versions are available, as consumers do not always upgrade their devices when new versions are

⁵⁴ <https://cyber-itl.org/2019/08/26/iot-data-writeup.html>

⁵⁵ <https://www.gov.uk/government/publications/pledges-from-industry-to-implement-iot-security-code-of-practice/pledges-from-industry-to-implement-iot-security-code-of-practice>

released. Some consumers may wait until a product stops physically working before replacing it, even if the product has been unsupported by security updates for some time.

50. The problem of legacy products will only get worse in the future if manufacturers continue to produce insecure products, and consumers are not aware of when their product is no longer supported by security updates. A 2019 survey found that the top three disposal methods for consumer IoT products were giving the product to a family or a friend, keeping it at home, and reselling the product, with throwing the device away being the least popular option.⁵⁶

2l(i) - Progress in eliminating Universal Default Passwords

51. The UK consumer rights organisation Which? has been working extensively to investigate and address security issues in consumer connectable products. As part of their core product testing operation, Which? has been routinely assessing the privacy and security provisions of consumer connectable products for several years. Data from Which? investigations and the Which? consumer test programme between October 2019 and January 2021 concerning the security of 253 consumer connectable products found that 9.9% of assessed products featured default passwords. The work of Which? has identified default passwords in product classes spanning wireless cameras, smart plugs, smart doorbells, wifi routers, and printers.
52. Other research suggests, based on a sample of 270 devices, that at least 4.7% of devices on the market contain a default password.⁵⁷ These products were identified as having a default password through explicitly stating this in their product manuals.
 - Other devices in this research were found to require the user to create a login or account before using the devices (78%). It is unclear from this research whether user-created passwords are required to be unique (and not easily guessable), and whether devices use these passwords once the initial set up is complete.
 - For the remainder of devices, it was not possible to determine if the device had a default password or not. Therefore, overall it was not possible to determine for 48% of the 270 devices whether or not they are sold with a default password.⁵⁸
 - It is important to note that this study only reviewed products that were sold by one UK retailer, and therefore only provides a partial picture of the broader landscape.
53. In addition to this, a recent (late 2020) Ipsos MORI survey commissioned by DCMS revealed that only one in five consumers check their devices for default passwords, suggesting that efforts by the UK Government via publishing consumer guidance and pushing manufacturers to provide more information to consumers about products are not impacting user behaviour. This highlights the need for regulation so that responsibility for improving the security of products is taken away from consumers.⁵⁹

2l(ii) - Prevalence of Vulnerability Disclosure Policies

54. Although work has previously been undertaken to develop best practices for vulnerability disclosure through voluntary International Standards Organization (ISO) standards⁶⁰, evidence suggests that a significant amount of consumer connectable product manufacturers have not fully embraced the principles underlying coordinated vulnerability disclosure.
55. Research conducted by the Internet of Things Security Foundation has found that many manufacturers still do not have a vulnerability disclosure policy in place. Of a total of 330 global manufacturers that were surveyed in 2019, only 13% reported that they had a vulnerability disclosure policy, a 3% increase from 2018 (90% of companies in 2018 vs. 87% in 2019 reported not having a policy in place).⁶¹ 18.9% of those surveyed in 2020 reported having a vulnerability disclosure policy. Although an improvement, this demonstrates that a significant majority of global manufacturers do not have robust systems in place to enable the reporting of identified vulnerabilities.
56. The absence of mechanisms by which vulnerabilities can be reported to manufacturers will limit their ability to identify and resolve these vulnerabilities. Data from Which? investigations and the Which? consumer test programme between October 2019 and January 2021 concerning the security of 253 consumer connectable

⁵⁶ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019

⁵⁷ Blythe, J.M., Sombatrung, N., Johnson, S., 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? <https://osf.io/preprints/socarxiv/63zkt/>. It is important to note that this study was based on well known UK brands and is therefore not representative of all devices sold within the UK market.

⁵⁸ Blythe, J.M., Sombatrung, N., Johnson, S., 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? <https://osf.io/preprints/socarxiv/63zkt/>

⁵⁹ 'Attitudes Towards IoT security', Ipsos Mori, which is to be published March 2021.

⁶⁰ ISO/IEC 291471 and ISO/IEC 301112 <https://www.iso.org/home.html>

⁶¹ IoTTF, 2020. Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report.

<https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTTF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf>

products found significant vulnerabilities or failures (ranging from low impact issues to critical flaws posing a significant risk to consumers) in all but two of the product types investigated.

2I(iii) - Prevalence of timely software updates, and transparency on how long products will receive security updates for

57. Data from the Which? consumer test programme and their other investigations into consumer connectable product security (October 2019 - January 2021) spanning 253 consumer connectable products identified only four (1.6%) products where clear information was provided (for an individual product, or at a brand level) on how long products will receive security updates for.
58. A review of 270 products for information on security updates found that across all of the products sampled, there was no indication of how long security updates would be provided.⁶² It is therefore difficult for consumers to distinguish between products with high and low quality security features at the point of purchase. This makes it difficult for consumers to assess products based on the quality of the security features built into the product.
59. Research conducted by the consumer group Which? has shown that 42% of active Android users worldwide are using smartphones with versions 6.0 or earlier. However, Android versions below 7.0 reportedly did not receive a security update throughout 2019. Tests conducted on five examples of smartphones, three years or older, and which were operating using Android software 8.0 or below, found that all of these smartphones were vulnerable to some types of malware, and in some cases multiple different types.⁶³
60. Furthermore, a survey conducted by Which? in March 2020 reported that 69% of Which? members expected their smart domestic appliances to last as long as non-smart versions of the product. On average, dishwashers and washing machines are expected to last 10 years, while fridges and tumble dryers are expected to last 11 years. Despite these long lives, Which? found that of the leading brands they asked, few were able to provide details of minimum software update support periods. Samsung reported a minimum update period of 2 years, while Beko confirmed a maximum update period of 10 years. On the other hand, Miele was the only brand who provided a clear policy, committing to a 10 year security update support period for their smart appliances.⁶⁴

2J - What sectors / markets / stakeholders will be affected, and how, if the government does intervene?

61. DCMS have identified 170 UK manufacturers and 3,485 retailers that will be directly affected by the PSTI Product Security measures.⁶⁵ This legislation will place proportionate duties on a range of key economic actors to ensure that insecure consumer connectable products are not made available to UK customers (See [5B - Description of preferred option](#) for further details). Manufacturers of consumer connectable products will be required to ensure that they implement a minimum security baseline in relation to products made available to UK customers. The number of UK retailers that will be affected is less clear but the number of specialised stores for the retail sale of electrical household appliances has been used as a best estimate.⁶⁶ The introduction of this regulation may result in a number of additional costs for both manufacturers and retailers such as: self-assessment costs; familiarisation costs; costs directly resulting from the implementation of the security requirements that represent the minimum security baseline; costs associated with creating a statement of compliance; as well as costs resulting from the disposal of non-compliant goods.

Section 3 - Rationale for intervention

62. The Government wants to ensure that the UK is one of the most secure places in the world to live and do business online, and has committed to ensuring that the majority of online products and services coming into use become 'secure by default'.
63. To support these aims, the government wants to ensure that consumers are able to use consumer connectable products as safely as possible, without the burden of having to implement security features within their products. However, as detailed above, a large number of consumer connectable products continue to be sold in the UK without basic cyber security provisions, despite the publication of best practice

⁶² Blythe, J.M., Sombatrung, N., Johnson, S., 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? <https://osf.io/preprints/socarxiv/63zkt/>

⁶³ <https://www.which.co.uk/news/2020/03/more-than-one-billion-android-devices-at-risk-of-malware-threats/>

⁶⁴ <https://www.which.co.uk/news/2020/06/the-truth-behind-smart-appliance-security-updates/>

⁶⁵ <https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/>

⁶⁶ <https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/>

guidance, leaving networks and infrastructure, consumers, and businesses vulnerable to the impacts of cyber security breaches.

64. The Government now believes that the insufficient progress that has been made in addressing these issues substantiates fundamental market failures that inherently limit the ability of the market to resolve this issue without additional government regulation. Manufacturers face a lack of economic incentives to build security into their devices for a number of reasons, which are detailed in the remainder of this section.

3A - Externalities

65. Externalities occur when costs or benefits associated with the production or consumption of a good or service are borne by a third party, who were not involved in the initial activity. In the case of consumer connectable products, there are wider costs to society associated with an insecure product becoming compromised.
66. The costs of cyber attacks enabled by insecure consumer connectable products often are not borne by the manufacturers or consumers of these products. Due to the network effect of connectable product security, a single vulnerability can compromise an entire network if it is exploited⁶⁷⁶⁸. Therefore, fewer insecure products connected to the internet (or connected to products that connect to the internet) would reduce the risk of cyber attacks enabled by vulnerabilities in these products, including wide scale botnet attacks, leading to a safer UK network for all consumers. Further details on botnet attacks are provided in the preceding section [2D - Botnets, and the impact of insecure consumer connectable products on networks and infrastructure](#).
67. As the full economic cost of attacks are not borne by the manufacturer or the consumer, these economic actors are therefore not incentivised to improve the security of their products in order to reduce the likelihood of these negative impacts occurring. The negative society-wide impacts of these externalities are further exacerbated by information asymmetry within the market.

3B - Information Asymmetry

68. Information asymmetry is a situation in which one party, taking part in the same economic transaction, has more information than another. In the consumer connectable product market, manufacturers possess more information than consumers about the security of the products that they produce and sell.
69. Research suggests that there is currently a significant lack of information provided to consumers on the built-in security provisions for connectable products.⁶⁹ This is despite the fact that nine in ten (87%) consumers believe that smart devices should have basic embedded features to protect user privacy and security and almost half (49%) of consumers report that security features are important to their decision making process when buying a smart device.⁷⁰⁷¹ Details of the evidence in this space are provided in the preceding section - [2H\(iii\) - Prevalence of timely software updates, and transparency on how long products will receive security updates for](#).
70. Moreover, 72% of the consumers that did not rank 'security features' in their top four considerations when buying smart devices (3,317 of 6,482 participants), stated this was because of an expectation that security was already built into devices.⁷² This indicates that many consumers are unaware of the security standards in consumer connectable products. Consequently, consumers are not able to demand a higher level of security from manufacturers of these products.
71. In many cases the owner of a compromised consumer connectable product may not realise that their product has been compromised, as, in many instances, compromised products may continue to function normally, and may not appear to be directly impacted by an attack, for example, when compromised devices are recruited into botnets (see the preceding section - [2D - Botnets, and the impact of insecure consumer connectable products on networks and infrastructure](#) for further details). Despite the scale of the potential cost to society, owners of insecure products may not see the link between insecurities embedded within their personal product and large scale external attacks. Consequently consumers may undervalue the benefits of a more secure product.

⁶⁷ Heartfield et al. (2018). A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home. Computers & Security, Vol 78

⁶⁸ <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#preventmalwaredelivery>

⁶⁹ Blythe, J. M., Sombatrung, N., & Johnson, S., 2018. 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?' <https://osf.io/preprints/socarxiv/63zkt/>

⁷⁰ Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

⁷¹ Harris Interactive, [Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019](#).

⁷² Harris Interactive, [Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019](#).

72. As a result of this information asymmetry, consumers do not have the knowledge to be able to make informed purchasing decisions, leading to consumers unwittingly putting themselves at risk of cyber attack through owning insecure products.

3C - Misaligned Incentives

73. The characteristics of the fast-moving and highly competitive technology market mean that security is not always built into consumer connectable products at the design stage. Instead, many manufacturers have taken a reactive approach to security. Manufacturers may not implement fixes for vulnerabilities in their products until these vulnerabilities have been discovered by external entities such as security researchers, or other technical experts.⁷³
74. One possible reason for this is the cost associated with building in security at the product development phase, as well as managing a vulnerability disclosure policy and providing security updates. This may require manufacturers to hire additional expertise or redesign software or hardware, leading to increased production costs and resulting in products becoming less price competitive. As a result, there are limited profit incentives for manufacturers to embed cyber security when developing their connectable products, except potentially increasing their market reputation.⁷⁴
75. Competitive pressures in this quickly evolving market also drive manufacturers to be the first to release new products onto the market, in order to gain an advantage over their competitors and capture a greater market share. Therefore, the implementation of security features may be overlooked in favour of functionality, device size or marginal cost savings.⁷⁵
76. Whilst the safety of consumer products (including consumer connectable products) is already subject to a regulatory framework in the UK, this is not the case for the security of these products. This means that manufacturers have an incentive at present to overlook cyber security concerns.

3D - Summary of Market Failures

77. Overall, the net effect of these factors mean that there are currently a lack of incentives for manufacturers to develop secure consumer connectable products, while consumers have a lack of knowledge, as well as a lack of available information, to enable them to make informed choices when purchasing new connectable products. This has led to an underinvestment in basic security measures being built into consumer connectable products by manufacturers (See the preceding section - [2H - Prevalence of baseline security measures](#) for further details).

⁷³ <https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/>

⁷⁴ The Internet Society, 2019, [The Economics of Consumer IoT Security](#).

⁷⁵ <https://enterpriseiotinsights.com/20180418/channels/analyst-angle/analyst-angle-the-race-to-the-bottom-security-problem-of-iot-Tag9>

Section 4 - Policy objective

78. The objective of this policy is to reduce the risk to consumers, networks, businesses and infrastructure of the range of possible harms that may arise from vulnerabilities and inadequate security measures in consumer connectable products. In taking action to reduce the risks that these products present, we hope to achieve the following effects:
- **Protect consumers, networks, businesses and infrastructure from harm.** Insecure connected products can be used by hostile actors to steal data, seize control of equipment and cause other harms.
 - **Enable emerging tech to grow and flourish** by improving security, and increasing consumer confidence.
 - **Demonstrate the UK's continued global leadership in cyber security.** The Code of Practice we published in 2018 has been adopted by many countries across the world and influenced international standards. This policy builds on the principles we outlined in the Code of Practice, and will allow us to continue to take a leadership role in this area. This includes leading the development of global standards and ensuring that these standards are applied and enforced.
 - *Since publishing the Code of Practice, our work has been amplified by the Five Eyes (UK, US, Canada, Australia and New Zealand). In 2019, the Home Secretary published the 'five country ministerial statement' outlining a Five Eyes commitment to collaborate and share evidence and align Five Eyes approaches to improving the security of consumer connectable products in our respective domestic markets. The statement sets out a principles-based approach to achieving improved security and was the product of the IoT Five Eye working group, which the UK continues to chair.*
 - *Governments of Australia (2020)⁷⁶ and India (2021) have published draft Codes of Practice with the same thirteen principles as those we published in 2018⁷⁷. In addition, the Singaporean voluntary labelling scheme and Finland's national consumer IoT certification scheme are based on EN 303 645, which was developed with input from DCMS.*
 - *The UK and Singapore also published a joint statement in 2019 on the internet of things, between the NCSC and representatives from Singapore's Cyber Security Agency⁷⁸.*
 - *We have been working as members of the IoT Security Platform, together with members from industry and foreign governments, including Arcep (France), ISED (Canada), MCTPEN (Senegal), AGESIC (Uruguay), METI (Japan), New Zealand, NIST (USA), The Internet Society and the Mozilla Foundation.*
 - *As evidenced in the case studies in [Box 4](#) and [Box 6](#), insecure consumer connectable products have been used by attackers to launch DDoS attacks on prominent businesses such as Amazon. This has resulted in websites being unavailable and disruption to customers. It is possible that similar attacks could be launched against the UK government. Therefore, addressing insecurities in consumer connectable products that allow them to be used in these attacks could benefit national security.*
79. As referenced in the preceding section - [2G - Previous UK Government Interventions](#), this work sits as part of a broader project that the Government has undertaken since the Secure by Design review was first launched in December 2016. 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 period⁷⁹ and builds on the existing NCSC technical guidance to industry published in May 2017.⁸⁰
80. The following sections detail the preferred intervention, as well as other policy options considered. Based on the extensive evidence compiled, and due to the market failures outlined above, further regulation is the only way to ensure that all new products entering the UK market include baseline cyber security provisions.

⁷⁶ <https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf>

⁷⁷ https://www.tec.gov.in/pdf/Whatsnew/Code%20of%20Practice_Consumer%20IoT.pdf

⁷⁸ <https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement>

⁷⁹ 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

⁸⁰ NCSC website on secure by default, 2017, accessed at: <https://www.ncsc.gov.uk/articles/secure-default>

Section 5 - Description of shortlisted interventions, preferred option, and plan for implementation

5A - Shortlisted policy interventions

81. Extensive engagement with key stakeholders and subject matter experts, consultations with industry, analysis of available evidence, and the collection of bespoke data informed the selection of the following policy options for shortlist appraisal:
 - **Option 0** - Do Nothing (counterfactual)
 - **Option A** - Voluntary security labelling scheme (Do-minimum option)
 - **Option B** - Mandatory security labelling scheme (Other viable option)
 - **Option C** - Legislating to ensure that consumer connectable products made available to UK customers comply with a minimum security baseline, initially aligned to the top three guidelines set out in the Code of Practice for Consumer IoT Security (Preferred option)
82. Further details of the policy development process that informed the selection of the shortlisted options can be found in [Annex 2 - Description of the policy development process, and other policy options considered](#).
83. Whilst key components of the intended legislative framework will be defined as part of the secondary legislation development process, DCMS has analysed the likely impacts of the shortlisted options in as much detail as possible for the purposes of this primary legislation impact assessment. Our rationale to justify the level of analysis used in this impact assessment, as well as further details of how DCMS will build upon this analysis in subsequent impact assessment publications, can be found in [Section 6 - Proportionality approach](#).

5A(i) - Option 0 - Do Nothing (counterfactual)

84. Policy options carried forward for shortlist appraisal have been assessed against a 'do nothing' counterfactual option, in which the UK Government would not intervene to reduce the risk to consumers and the wider economy of insecure consumer connectable products.
85. It should be noted that, in contrast to the consultation stage impact assessment published in 2019 for this work, this baseline scenario is separated from the scenario in which the government would introduce a voluntary labelling scheme (Option A), to enable an assessment of the impacts of this non-legislative option relative to the shortlisted legislative interventions (Options B and C).
86. The consultation stage impact assessment noted that the EU Cybersecurity Act would establish an EU cyber security certification framework when enacted, under which cyber security certification schemes across the EU, including any IoT certification schemes, would be harmonised. Awaiting the outcome of this possible harmonisation activity and subsequently adopting a consumer IoT certification scheme was cited as one option for addressing the risks posed by insecure consumer connectable products.
87. Following the publication of the consultation stage impact assessment, the EU Cybersecurity Act entered into force on 27 June 2019. Title III of the Cybersecurity Act sets out a Cybersecurity Certification Framework. The framework will enable the creation of certification schemes for different categories of ICT products, processes and services⁸¹, however, concrete details of any efforts to develop an IoT certification framework have not yet emerged.
88. There is not yet sufficient information available about the details of any future EU efforts to regulate the cyber security of consumer connectable products (through a harmonised certification framework or otherwise) to be able to model the possible impact of businesses having to comply with both EU and UK regulatory schemes for the purposes of this impact assessment. The Government will continuously review the intended legislative framework in the context of broader regulatory changes to ensure it remains effective and proportionate, and will model any duplication of burden from complying with both UK and EU regulations as appropriate in any future impact assessment publications as appropriate.

5A(ii) - Option A - Voluntary Security Labelling Scheme

89. This non-regulatory option would attempt to address the failure of information asymmetry regarding the security of consumer connectable products.

⁸¹ <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity>

90. Under this intervention, manufacturers of consumer connectable products would be able to voluntarily use a security label, which would help consumers to determine whether a product complies with a security baseline aligned to the top three Code of Practice guidelines.
91. Manufacturers who opted to participate in the scheme would have to indicate through either a positive or negative label whether the product adheres to the security baseline. The label would also need to include details of the minimum length for which the product will be supported with security updates.
92. Consumers would be able to use information provided in the label to consider the security features of a product when making a purchasing decision. Evidence suggests that individuals who value security will demand more secure products, which could incentivise manufacturers to build basic security provisions into their products, addressing the market failure of misaligned incentives. In the long run, as more products become more secure and manufacturers take into account device security in the design phase of their product's development, the wider UK economy would become more secure.
93. It should be noted that for this intervention, a consumer's willingness to purchase a device with a positive label would depend on both the uptake of the voluntary label, and the availability of close substitutes. Products with a positive label may not meet the consumer's requirements, leading them to choose unlabelled products instead, should they value cost and functionality more than security.⁸²

5A(iii) - Option B - Mandatory Security Labelling Scheme

94. This regulatory option would attempt to address the failure of information asymmetry regarding the security of consumer connectable products by mandating that all consumer connectable products made available in the UK feature a security label.
95. Manufacturers of consumer connectable products would be obligated in legislation to use a physical security label on their product's packaging, evidencing the extent to which the product complies with a security baseline aligned to the top three Code of Practice guidelines.
96. Retailers of consumer connectable products in the UK market would also be responsible for ensuring that the products that they sell display the correct security label. This could be through an information exchange between the manufacturer and retailer, or through gaining assurance that the product meets the security baseline.
97. As detailed in [Annex 2E - Development of labelling scheme options](#), DCMS has undertaken extensive work to analyse the likely efficacy of both a voluntary and mandatory labelling scheme.
 - DCMS undertook work with the PETRAS Consumer Security Index Project to fund and compile a rapid evidence assessment on labelling schemes for IoT security.^{83,84} This included DCMS part-funding 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.⁸⁵
 - An iterative approach was taken with a range of stakeholders, including via workshops, to initially gather views on various approaches for a labelling scheme. Research on the impact of labels on consumer choice was also conducted, including testing different labelling designs.⁸⁶

5A(iv) - Option C - Legislating to mandate a minimum security baseline for consumer connectable products

98. Details of the preferred policy option are captured in [5B - Description of preferred option](#). In summary, the intended intervention will:
 - introduce a legislative framework to enable Ministers to mandate a minimum security baseline for consumer connectable products that can be updated over time to remain effective in the face of broader technological or regulatory changes;
 - mandate that all manufacturers of consumer connectable products making their products available ensure that these products comply with a minimum security baseline specified by Ministers, which would initially align to the top three Code of Practice guidelines;

⁸² Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019

⁸³ 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>

⁸⁴ Make It Clear, 2019. [DCMS- IoT labelling online study](#).

⁸⁵ 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/>

⁸⁶ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.

- mandate that retailers, importers and distributors involved in the transmission of consumer connectable products to customers play a role in ensuring that these products meet the minimum security baseline;
 - ensure that UK manufacturers share information with relevant economic actors regarding the compliance of consumer connectable products, through self-declaring their compliance or seeking third-party certification; and
 - set out how the legislation will be enforced.
99. The three initial security requirements that the Government is proposing to mandate as part of the initial minimum security baseline have been selected following extensive feedback from industry, academia and other stakeholders. This involved conducting a consultation on our regulatory approach (see [Annex 2B - May 2019 consultation on consumer IoT security regulatory proposals](#)) followed by a call for views on our detailed regulatory proposals (see [Annex 2D - July 2020 call for views on proposals for regulating consumer connectable product cyber security](#)).

5B - Description of preferred option

100. DCMS has collaborated with NCSC, international partners, industry, academia, cyber security experts, and civil society in developing its intended intervention (Option C), which is to regulate consumer connectable product cyber security through legislation. The legislation will enable Ministers to specify a minimum cyber security baseline that key economic actors involved in making consumer connectable products available to UK consumers will be obligated to ensure that these products comply with.
101. Initially this minimum cyber security baseline will align to the top three guidelines from the Code of Practice for Consumer IoT Security, and key provisions within ETSI European Standard (EN) 303 645. However, the planned legislation will enable Ministers to adapt this baseline over time, to ensure the legislation remains effective amidst changes to the wider regulatory, technical or threat landscapes.
102. The legislation will place proportionate obligations on relevant economic actors involved in the manufacture and distribution of consumer connectable products, and establish a robust enforcement regime to achieve this outcome.
103. The twelve key policy positions that underpin the PSTI Bill Product Security measure are summarised in [Box 9](#). Further details of these positions are available as part of the 2021 Government response to its call for views on consumer connectable product cyber security regulatory proposals⁸⁷.

Box 9 - Key details of policy positions underpinning the preferred intervention (Option C)

Scope of the PSTI product security measures

Key Policy Position 1 - Detailing products in scope

The legislation will apply to any network-connectable devices and their associated services that are made available primarily to consumers, except products that are designated as out of scope.

- *The legislation will only apply to products intended to be used by consumers, or products that are likely to be used by consumers in reasonably foreseeable conditions. This will include products primarily used by consumers, but that can also be used in a business environment such as Smart TV's or connected security cameras, but exclude products that are only used by businesses or in industrial settings. The risks associated with products only used by businesses or in industrial settings are being reviewed as part of a separate programme of work.*
- *The legislation will only apply to products that have a network interface (e.g. can communicate data via Wifi, Bluetooth, data cable etc.). This includes "ancillary" products that connect primarily to other devices.*
- *The legislation will apply to both devices and their associated services (see [products in scope and key terminology](#) for details of how best to interpret these terms).*
- *Wherever practical, the legislation will apply to all activity that could lead to*

⁸⁷ Government response: Call for views on proposals to regulate consumer connectable product cyber security, 2021 - available at the Secure by Design GOV.UK collections page: <https://www.gov.uk/government/collections/secure-by-design>

vulnerable products being made available to consumers, including consumer connectable products that are:

- both free of charge and paid for;
- sold in shops both online and offline;
- offered as incentives or free sign up gifts as part of a contract for offer / promotion;
- in exchange for promotion;
- financed products that a consumer will own once all payments have been made;
- made available as part of an insurance contract; and
- traded for another good or service.

Key Policy Position 2 - Exempted product classes

Specific product classes that would otherwise fall within the scope of this legislation, but for which it would be inappropriate for it to apply, will be excepted from the legislative framework.

- *To ensure businesses are not subject to an unnecessarily duplicative regulatory regime, product classes that are subject to comparable regulation, either currently or in the near future, will be excepted at the point where the legislation is commenced, including some **Smart Meters** and certain categories of **Automotive vehicles**.*
- *Products that the Government has deemed inappropriate to include pending further investigation will also be excepted at the point where the legislation is commenced, including **desktop computers, laptops, and tablets without a cellular connection**.*
- *Products where inclusion would impose impractical obligations on business will also be excepted from scope at commencement. This chiefly applies to **second-hand products**.*

Key Policy Position 3 - Adaptable scope

Where changes to the wider regulatory, technological, or threat landscapes render it appropriate, the legislation will allow Ministers, subject to agreement by Parliament, to adjust the scope of consumer connectable products covered by the regulation, by updating the list of specific product classes excepted from its effects.

Key Policy Position 4 - Interoperability

The legislation will be interoperable with other existing or planned government interventions covering contiguous, or overlapping product classes.

- *For example, the PSTI product security measures will be compatible with the Department for Business, Energy & Industrial Strategy commitment to regulate smart appliances, including their interoperability, data privacy and cyber security.⁸⁸*

Role of economic actors

Key Policy Position 5 - Obligations on economic actors

The legislation will place proportionate obligations on relevant economic actors involved in the manufacture, import and distribution of in scope products to consumers to ensure that insecure products are not made available on the UK market.

- *Manufacturers of consumer connectable products will be obligated to comply with duties including the following:*
 - *Comply with the minimum security baseline outlined in legislation through security requirements with respect to consumer products intended to be*

⁸⁸ Energy white paper: Powering our net zero future, HM Government, 2020
<https://www.gov.uk/government/publications/energy-white-paper-powering-our-net-zero-future>

made available to UK customers.

- *Only make such products available alongside a statement of compliance;*
- *Take action if they make a product available where there is a compliance failure.*
- *For products made by manufacturers based outside of the UK, certain manufacturer obligations will fall to the manufacturer's authorised representative, should an appropriate authorised representative exist.*
- *Economic actors involved in the distribution of in scope products to consumers (including wholesalers and retailers) will be obligated to comply with duties including the following:*
 - *Verify that the manufacturers of consumer connectable products the retailer is involved in the transmission of have published a statement of compliance.*
 - *Take action if they make a product available on the market in relation to which there is a compliance failure.*

Key Policy Position 6 - Security Requirements

The legislation will obligate relevant economic actors to not make consumer connectable products available on the UK market unless they comply with a mandatory security baseline.

- *The intended legislative framework will feature two routes to conformity. The first route is to implement the security requirements as detailed in legislation. These initial security requirements have been derived from and align with the top three guidelines from the Code of Practice for Consumer IoT Security.*
- *As a second alternative route to conformity, the legislative framework will also designate specific provisions / clauses of relevant external standards where the implementation of these achieves the same (or nearly the same) outcome as implementation of the security requirements detailed in legislation.*
- *Relevant economic actors will be obligated to not make consumer connectable products available on the UK market unless they comply with the security requirements as detailed in the broader legislative framework.*
- *The initial security requirements will align to the top three guidelines from the Code of Practice for Consumer IoT Security and key provisions within the ETSI EN 303 645:*
 - *Security Requirement 1 (Ban universal default passwords) - covering all passwords within the device, including those not normally accessible to the user, and pre-installed software applications, including those that are 3rd party provided but pre-installed on the device. Easily guessable or derivable passwords will also be banned.*
 - *Security Requirement 2 (Implement a means to manage reports of vulnerabilities) - a vulnerability disclosure policy that covers the relevant product will need to be publicly available.*
 - *Security Requirement 3 (Provide transparency on how long, at a minimum, the product will receive security updates) - The minimum length of time that a product will receive security updates should be published.*

Key Policy Position 7 - Adaptable security requirements

Where changes to the wider regulatory, technological, or threat landscapes render it appropriate, the legislation will allow Ministers to update the security requirements that relevant economic actors must ensure products made available on the UK market comply with.

- *This would be done in circumstances where such action was necessary to keep pace with changes to the wider regulatory, technological, or threat landscapes. In the future, it may be necessary to introduce requirements relating to (but not limited to) areas such as the following:*
 - *User authentication*
 - *Vulnerability reporting*
 - *Software updates*
 - *Protection of data at rest and in transit*
 - *Security design principles for software and hardware*

- *Protection of personal data (privacy)*
- *Product and wider network resilience*
- *Provision of information and guidance to product users*

Key Policy Position 8 - Product Assurance

Where changes to the wider technological or threat landscapes render it appropriate, the PSTI product security measures will enable Ministers to mandate product assurance for particular categories of consumer connectable products.

- *Undergoing an assurance process will not be mandated for any consumer connectable product classes at the point where the PSTI product security measures come into force, but the legislation will allow product assurance to be subsequently mandated for specific consumer connectable product classes if changes to the wider technological or threat landscapes render it appropriate.*

How the legislation will be enforced

Key Policy Position 9 - Enforcement authority

An enforcement authority will investigate non-compliance, take action in relation to any non-compliance, and provide support to relevant economic actors to enable them to comply with their obligations.

Key Policy Position 10 - Enforcement role and responsibilities

To enable proportionate enforcement across a range of contexts, the legislation will equip the enforcement authority with necessary powers, as well as the ability to issue appropriate corrective measures and sanctions.

Key Policy Position 11 - Appeals

Relevant economic actors will have the right to appeal any sanctions or corrective measures brought against them, in a manner consistent with the processes used in existing product safety legislation.

Key Policy Position 12 - Proportionate transitional provisions

Following royal assent, the Government will provide relevant economic actors with an appropriate grace period to adjust their business practices before the PSTI product security measures fully comes into force.

- *The Government is committed to ensuring that businesses are given an appropriate amount of time to adjust their business practices before the legislation is actively enforced.*
- *Whilst specific timings are subject to change, active enforcement of this legislation is likely to commence no earlier than one year following royal assent.*

5C - How the preferred option will be given effect

104. Unpredictable changes to the wider technological, threat and regulatory landscapes, such as the rapid emergence of new product classes, the identification and exploitation of new vulnerabilities, or the emergence of overlapping regulatory interventions, could limit the effectiveness of the PSTI product security measures.
105. It is critical that the preferred intervention remains effective in reducing the risk of the harms that may arise from vulnerabilities and inadequate security measures in consumer connectable products over time, even amidst potential changes to the broader landscape. To enable the Government's approach to adapt to such changes, specific elements of the legislative framework will be defined in secondary legislation.
106. The primary legislation that this impact assessment principally relates to is the product security measures in the PSTI Bill. In summary, this legislation will create a robust and adaptable framework for regulating consumer connectable product cyber security by:
 - **defining products in scope of the legislative framework;**

- **defining the economic actors that will need to take action** to protect consumers from insecure consumer connectable products;
 - **defining the obligations** that relevant economic actors will be expected to comply with;
 - **defining key elements of the enforcement approach**, including powers, corrective measures and sanctions available to the appointed enforcement authority; and
 - **providing powers to the Secretary of State** to set out or update key elements of the legislative framework using necessarily more agile mechanisms, such as in secondary legislation.
107. The legislation will also provide the Secretary of State with the power to delegate their enforcement powers to another enforcement authority.
108. Following the Royal Assent of the PSTI Bill, secondary legislation may further detail and amend key components of the legislative framework such as the security requirements.
109. It should be noted that whilst best endeavours have been made to capture the full impact of the intended legislative approach in this impact assessment, the Government will produce additional impact assessment publications in the future, which will further detail the impact of elements of the legislative framework defined as part of the secondary legislation development process. Further details of the analysis undertaken in this impact assessment are available in the subsequent section - [6A - Extent of analysis and further impact assessment publications](#).
110. To ensure that the PSTI product security measures remain effective over time in protecting consumers and the economy from security vulnerabilities in consumer connectable products, the Government may bring forward additional secondary legislation in the future to update key elements of the legislative framework, if rendered appropriate by changes to the wider technological, regulatory, or threat landscapes (See [Box 9](#) for further details of the intended legislative framework, and steps the Government is taking to ensure it remains effective over time).

5D - How the intervention would meet our policy objectives

111. The core objective of this intervention is to reduce the risk to consumers, networks, businesses and infrastructure of the range of possible harms that may arise from vulnerabilities and inadequate security measures in consumer connectable products.
112. The view of NCSC - the UK's technical authority for cyber threats, is that compliance with the initial minimum security baseline that the intended legislative framework will mandate, will "*make the most fundamental difference*" to the cyber risks posed by these products (see [NCSC statement 1](#)), and "*reduce the threat of cyber attacks to consumers*" (see [NCSC statement 3](#)).
113. The initial minimum security baseline will reduce the risk of the harms that may arise from vulnerable consumer connectable products by:
- **Ban universal default passwords** - eliminating a key vulnerability which can enable cyber criminals to attack affected product classes at scale. This requirement will make it substantially harder for an attacker to build large botnets from new devices that enter the market, and will reduce the likelihood that individual devices would be compromised to cause harm to individuals.
 - **Implement a means to manage reports of vulnerabilities** - ensuring that the public and security research community is able to inform manufacturers of vulnerabilities they identify, so that they can be fixed.
 - **Provide transparency on how long, at a minimum, the product will receive security updates** - ensuring that, when buying a product, consumers know how long it will be supported with security updates for, enabling them to make more informed decisions about the risks of these products.
114. Compliance with the initial security baseline would therefore be evidence that this intervention had met our core policy objective.

5E - When will the arrangements come into effect

115. The Government's intention is for this legislation to come into force as soon as is practicable, whilst providing relevant economic actors with an appropriate grace period to adjust their business practices. Whilst specific timings are subject to change, active enforcement of this legislation is likely to commence no earlier than one year following royal assent.

Section 6 - Proportionality approach

6A - Extent of analysis and further impact assessment publications

116. It is our view that the bringing into force of all primary and secondary legislation necessary to deliver the preferred option (as detailed in [5C - How the preferred option will be given effect](#)) would meet the threshold stipulated in the RPC proportionality guidance for a high impact measure, as a result of:
- the estimated EANDCB and NPSV for the preferred option both exceeding +/- £50 million;
 - the large number of businesses that will be affected;
 - the significant change to existing requirements the preferred option represents; and
 - the large number of factors that need to be considered to estimate the impact of the measure.
117. As far as possible in the context of the fundamental barriers to gathering representative evidence for some key cyber crime variables, we are therefore committed to ensuring that a detailed analysis of the total impact of our proposed intervention is made available for RPC scrutiny before elements of these measures that would impose any duties on businesses come into force.
118. In line with RPC guidance on the assessment and scoring of primary legislation measures, for the purposes of this impact assessment we have sought to provide an indicative view of the likely scale of impacts of the whole policy (across both primary legislation and all secondary legislation necessary for the bill to come into force), including an indicative cost benefit analysis of our shortlisted interventions, based on the significant evidence base gathered to date (See [Box 10](#) for further details):

Box 10 - Overview of the evidence base underpinning the indicative cost benefit assessment detailed in this impact assessment

For the indicative cost benefit analysis in this impact assessment, we have sought to establish as robust an evidence base as possible using a broad range of data sources, bespoke commissioned studies, and consultations to support the policy development process.

In parallel with our extensive collaborative policy development work with industry, cyber security stakeholders, civil society and academia detailed in the preceding section [2G - Previous UK Government Interventions](#), DCMS has convened multiple industry workshops, held a formal consultation in 2019 and a call for views on updated regulatory proposals in 2020, worked with international governments, and commissioned bespoke research, such as tasking external suppliers with conducting two business surveys and three consumer surveys.

DCMS has also consulted relevant non-for-profit organisations such as Which? to better understand key variables, including compliance levels with aspects of the minimum security baseline that the preferred option will seek to mandate. This work has also been supported by extensive additional engagement by NCSC and DCMS with industry to gather information and test assumptions.

119. Whilst we have sought to provide a robust analysis of the likely impacts of our measure as a whole in this primary legislation impact assessment, multiple elements of our broader legislative approach that are fundamental to understanding the total impact of the preferred option may be further defined in secondary legislation, as part of the secondary legislation development process, or otherwise following the royal assent of the PSTI Bill. These include the following:
- the list of products to be excepted from the scope of this regime;
 - the initial set of security requirements the measure will obligate relevant economic actors to comply with; and
 - the identity of the authority authorised by Ministers to act as the enforcement authority for this legislation.
120. As far as possible, this impact assessment attempts to estimate the impact of the whole policy, based on our existing view of the most likely shape of secondary legislation required to commence the PSTI product security framework overall. [Box 11](#) contains an overview of some matters that may be adjusted as part of the secondary legislation development process.

Box 11 - Key policy decisions to be taken after the primary legislation development process

Adaptable scope

As detailed in [5B - Description of preferred option](#), the product security measures in the PSTI Bill allow the Secretary of State to update the scope of products this legislation will apply to. The legislation will enable the Secretary of State to manage a list of excepted products that would otherwise fall within the scope of our definition of these measures, to ensure that the legislative framework remains effective amidst changes to the wider regulatory, technological, or threat landscapes. This power will be deployed in instances where the balance of expert advice, robust analysis, and proportionate engagement leads the Secretary of State to the conclusion that the scope of products captured by this regulation must be modified. This power is also necessary to ensure this legislation aligns with evolving cyber security requirements that already cover certain product classes through other legislation.

Changes to the product classes this legislation will apply to will affect the extent of its direct impact on government, businesses, and consumers. For example, policy decisions taken as part of the secondary legislation development process on scope could conceivably change the indicative cost benefit analysis through altering:

- the anticipated benefits (reduced costs of cyber attacks);
- the total number of economic actors that will be subject to the obligations of this legislation, including specialist manufacturers and retailers of products that were not originally included in scope;
- the number of small and micro businesses that will be impacted by this legislation;
- the overall impact of this legislation on small and micro businesses relative to larger businesses, as small and micro businesses that specialise in the manufacture or distribution of specific product classes may have different characteristics (e.g average number of product lines, compliance rates); and
- the anticipated cost of enforcing the legislation.

Identity of the enforcement authority

As detailed in [5C - How the preferred option will be given effect](#), the legislation will allow the Secretary of State to delegate their enforcement powers to another enforcing authority. A number of considerations, developed in line with government best practice on appraisal and evaluation, and on which feedback was solicited in the July 2020 call for views, have been used to develop the methodology employed to consider whether to exercise these powers.

Different enforcement authorities vary in terms of relevant technical expertise, current staffing levels, and access to relevant capital such as testing facilities. The likely cost of enforcement will also depend on the scope of products that the legislation will apply to when it is brought into force, which itself is subject to change as part of the secondary legislation development process. For the above reasons, it would not be appropriate to attempt to definitively determine the likely cost of enforcing this legislation as part of the primary legislation development process.

121. As policy decisions that will determine key elements of the intended legislative framework will be taken after the conclusion of the primary legislation development process, DCMS will build upon the indicative cost benefit analysis in this impact assessment in future impact assessment publications, to ensure the impact of the total intervention has been analysed to an appropriate level of robustness for a high impact measure.
122. Whilst the cost benefit analysis provided in this impact assessment is indicative, and subject to change based on policy decisions made as part of the secondary legislation development process, we believe that the outputs of our indicative analysis clearly suggest that the EANDCB for the preferred option is likely to exceed the de minimis threshold (+/- £5 million). DCMS will therefore submit a further impact assessment publication for RPC scrutiny before tabling the secondary legislation necessary to bring the product security measures in the PSTI Bill into force.

6B - Proportionate analytical approach for indicative cost-benefit analysis

123. We have sought to conduct detailed analysis of the likely impacts of shortlisted options using the assembled evidence base, with sensitivity analysis being used to quantify key impacts subject to unavoidable uncertainty.

124. Using the gathered evidence, DCMS has been able to estimate the direct cost to key economic actors involved in the production and distribution of consumer connectable products that may result from the shortlisted options. These are outlined in section [7B\(iii\) - Estimating the cost of cyber attacks](#).
125. DCMS's approach to modelling the benefits of intervention arises from an assumption that implementation of the proposed security baseline will reduce the number of cyber attacks against consumers and businesses. The view of NCSC - the UK's technical authority for cyber threats, is that estimating the reduction in probability of a successful cyber attack resulting from the shortlisted interventions is "*inherently challenging*". NCSC has also noted that, as a result of the inherent complexities of identifying cyber attacks, "*there is no quantifiable evidence to be able to gauge or analyse crime specific to connected consumer devices*" (see [NCSC Statement 4](#) for further details).
126. Whilst DCMS has been able to gather evidence on the direct cost of the shortlisted interventions and estimate costs to both consumers and businesses relating to a cyber attack, there is a lack of available evidence on cyber crime specific to consumer connectable products, and the challenges noted in [NCSC Statement 4](#) have precluded DCMS from being able to gather bespoke evidence to fill this gap. Therefore, to estimate the potential benefits that would arise from the shortlisted intervention, the extent to which implementation of the security baseline would reduce the likelihood of cyber crime has been assumed. This assumption has been supported by (i) NCSC and (ii) sensitivity analysis.
127. In addition to this, a potential unintended consequence of policy option B and C is an increase in the disposal of consumer connectable products. Again, this is an area that is difficult to estimate because it requires an understanding of how businesses will respond to the proposals. For instance, as described in section [7E\(iv\) - Estimating the costs associated with the disposal of non-compliant goods](#), to avoid losing revenue it is possible that manufacturers and or retailers will sell non-compliant connectable products at a reduced price or sell into alternative markets (outside of the UK) rather than dispose of them. For the purposes of this impact assessment, an assumption has been made around the proportion of non-compliant stocks that may be disposed of (5%,10%,45%).

NCSC Statement 2

Estimating the costs of consumer connectable product disposal

"The NCSC supports DCMS's assessment that the cost associated with non-compliant connected products is an overestimate for the reasons set out above. The service Greynoise has seen approximately 1500 (between the 1st January and mid-February 2021) attempted attacks by Mirai infected devices on their sensors (using default passwords). However, this is one source and only paints a partial picture because of its focus on one particular type of malware. As noted in [NCSC Statement 1](#) and [NCSC Statement 5](#) it is very difficult to assess the number of attacks that occur on an annual basis related to vulnerable consumer devices."

128. Overall, DCMS has gone to great lengths to fill evidence gaps but due to the inherent challenges involved in identifying cyber crime; low response rates in DCMS commissioned surveys; or due to challenges associated with forecasting how businesses will respond to the proposals, some evidence gaps remain. In these instances, DCMS has used assumptions alongside the best available evidence in order to quantify the impact of the proposed policy options.

Section 7 - Indicative Cost-Benefit Analysis

129. This section provides details of the following:

- The **analytical approach** taken to assess the shortlisted policy interventions
- The **assumptions** used as part of this analysis, and justifications for those assumptions. For a complete list of the assumptions used throughout the impact assessment see [Annex 3 - Risks and Assumptions](#).
- The **outputs of modelling of the benefits and costs** that would result from the shortlisted policy interventions.

130. [Table 1](#) summarises the outputs of the Indicative Cost-Benefit model for the three shortlisted policy interventions (detailed in [5A - Shortlisted policy interventions](#)). It should be noted that the shortlisted policy interventions have been assessed against the 'do nothing' option. In contrast to the consultation stage impact assessment, the baseline scenario in this impact assessment assumes a pre-voluntary scheme status quo, allowing for a comparison to be made between the voluntary labelling scheme and the 'do-nothing' approach.

Table 1 - Summary of Indicative Cost-Benefit Analysis: 10 Year Net Present Value

Shortlisted policy option	Worst Case	Central Estimate	Optimistic Case
Option A (Do-minimum) Voluntary security labelling scheme	-£28.4m	£3.7m	£140.1m
Option B (Other viable option) Mandatory security labelling scheme	£-443.6m	£1056.1m	£6435.8m
Option C (Preferred option) Mandate a cyber security baseline aligned to the top three Code of Practice guidelines	£379.4m	£6807.5m	£16431.5m

131. The cost benefit analysis of the shortlisted policy options has been conducted in line with guidance from HMT Green Book. As such, a discount rate of 3.5% has been applied to future costs and benefits to account for the time preference of money. Inflation has been accounted for using HMT GDP Deflators and the base year for the analysis is 2020.
132. consumer connectable products are a relatively new area of technology, meaning that the true costs of insecure devices and services on the market have traditionally been and continue to be difficult to quantify. The Government has endeavoured to gather a proportionate evidence base for this impact assessment (see [Section 6 - Proportionality approach](#) for further details). Challenges, including inherent technical barriers (for instance, in quantifying instances of cyber crime) and low response rates (two surveys were sent to over 2,000 companies but only 22 consumer IoT manufacturers and 12 retailers responded) have necessitated the assumption of some variables for which there is remaining uncertainty. Despite the limitations of some of the data used, the figures presented in this impact assessment are based on the best available data.
133. Assessing the likely impact of the shortlisted policy interventions on consumers, businesses, and the Government has required the quantification of a number of costs and benefits, not all of which apply to every assessed intervention. [Table 2](#) summarises the component benefits and costs of each modelled policy intervention.

Table 2 - Overview of modelled costs and benefits per shortlisted policy option (central estimate)

Modelled benefits and costs	Option A <i>Voluntary label</i>	Option B <i>Mandatory label</i>	Option C <i>Mandatory baseline</i>
Impacts on consumers			
Benefit: Reduced cost of cyber crime enabled by insecure consumer connectable products	£29.1m	£1,146.2m	£6,881.1m
Impacts on manufacturers			
Cost: Familiarisation with the regulation	£0.27m	£0.27m	£0.42m
Cost: Self-assessment against the security baseline	£0.20m	£11.0m	£11.0m
Cost: Labelling		£5.8m	
Cost: Implementing security improvements			£30.4m
Cost: Publication of a statement of compliance			£2.2m
Impacts on retailers			
Cost: Familiarisation with the regulation	£24.6m	£24.6m	£68.8m
Cost: Disposal of non-compliant goods		£96.6m	£96.6m

Cost: Verification of a statement of compliance			£2.4m
Impacts on business users of consumer connectable products			
Benefit: Reduced cost of cyber crime enabled by insecure consumer connectable products	£6.8m	£389.6m	£1,798.6m
Impacts on government			
Cost: Enforcement		£7.2m	£7.2m

Table 3 - Overview of the direct and indirect impacts to businesses across the proposed policy options

	Option A <i>Voluntary label</i>	Option B <i>Mandatory label</i>	Option C <i>Mandatory baseline</i>
Costs			
Familiarisation cost	Direct Impact	Direct Impact	Direct Impact
Self-assessment cost	Direct Impact	Direct Impact	Direct Impact
Labelling cost	Direct Impact	Direct Impact	
Disposal of non-compliant goods		Direct Impact	Direct Impact
Declaration of conformity			Direct Impact
Verification of declaration			Direct Impact
Security Improvements			Direct Impact
Enforcement costs	Does not directly impact businesses	Does not directly impact businesses	Does not directly impact businesses
Benefits			
Benefits to individual consumers	Direct Impact	Direct Impact	Direct Impact
Benefits to businesses as consumers	Indirect Impact	Indirect Impact	Indirect Impact

7A - Structure of the Indicative Cost-Benefit Analysis

134. For ease, the Indicative Cost-Benefit Analysis has been organised according to the different types of costs and benefits quantified, and the relevance of the methodology adopted to the shortlisted options:

- **Section 7B - Underlying methodology of relevance to all options:** This section focuses on aspects of the modelling approach that are relevant to all shortlisted options before moving onto a discussion of the costs that are not relevant to all options:
 - [7B\(i\) - Estimating the number of consumer connectable products](#)
 - [7B\(ii\) - Estimating the replacement rate of consumer connectable products](#)
 - [7B\(iii\) - Estimating the cost of cyber attacks](#)
- **Section 7C - Benefits methodology of relevance to all options:** This section details the approach taken to estimating the benefits that would arise from implementing the shortlisted options, focusing on benefits that (to varying degrees) would arise in all of the shortlisted policy options:
 - [7C\(i\) - Estimating the benefits resulting from reduced cyber crime](#)
 - [7C\(ii\) - Non-monetised benefits](#)
- **Section 7D - Costs methodology of relevance to all options:** This section details the approach taken to estimating the benefits would arise from implementing the shortlisted options, focusing on benefits that (to varying degrees) would arise in all of the shortlisted policy options:
 - [7D\(i\) - Estimating the number of manufacturers and retailers of consumer connectable products](#)
 - [7D\(ii\) - Estimating familiarisation costs](#)
 - [7D\(iii\) - Estimating self-assessment costs](#)
 - [7D\(iv\) - Estimating costs to retailers](#)
- **Section 7E - Costs methodology not of relevance to all options:** This section details the approach taken to estimating the costs that would arise from implementing the shortlisted options, focusing on the costs that may be of specific relevance to one or two of the shortlisted options:
 - [7E\(i\) - Estimating the costs of labelling](#)
 - [7E\(ii\) - Estimating the costs of implementing security improvements](#)
 - [7E\(iii\) - Estimating the costs of publishing and verifying a statement of compliance](#)
 - [7E\(iv\) - Estimating the costs associated with the disposal of non-compliant goods](#)
 - [7E\(v\) - Estimating the costs of enforcement](#)

135. Details of additional analysis and tests the department has conducted are provided in [Section 8 - Additional Analysis](#). This includes the following:

- [8A - Analysis of the potential costs to consumers](#)
- [8B - Analysis of the impact on small and micro businesses](#)
- [8C - Break-Even Analysis](#)
- [8D - Analysis of potential trade impacts](#)
- [8E - Equalities Impact Assessment](#)
- [8F - Assessment of impact on innovation](#)

7B - Underlying methodology common to all options

7B(i) - Estimating the number of consumer connectable products

Estimating growth in the adoption of consumer connectable products

136. Adoption of IoT products in the UK is predicted to grow into the future, with some estimates predicting 156 million devices by 2024.⁸⁹ Forecasts suggest that there could be up to 50 billion connectable devices worldwide by 2030.⁹⁰ It is important to note that while forecasts often differ slightly due to differences in the definition of IoT (see [Section 1 - Products in scope and key terminology](#)), they all suggest that consumer connectable products are becoming increasingly common.
137. Research commissioned by Ofcom on the number of UK consumer IoT products has been used in this impact assessment to forecast the number of consumer consumer connectable products (with the exception of

⁸⁹ [Cambridge Consultants, 2017. Connected Nations Report 2017: Data Analysis.](#)

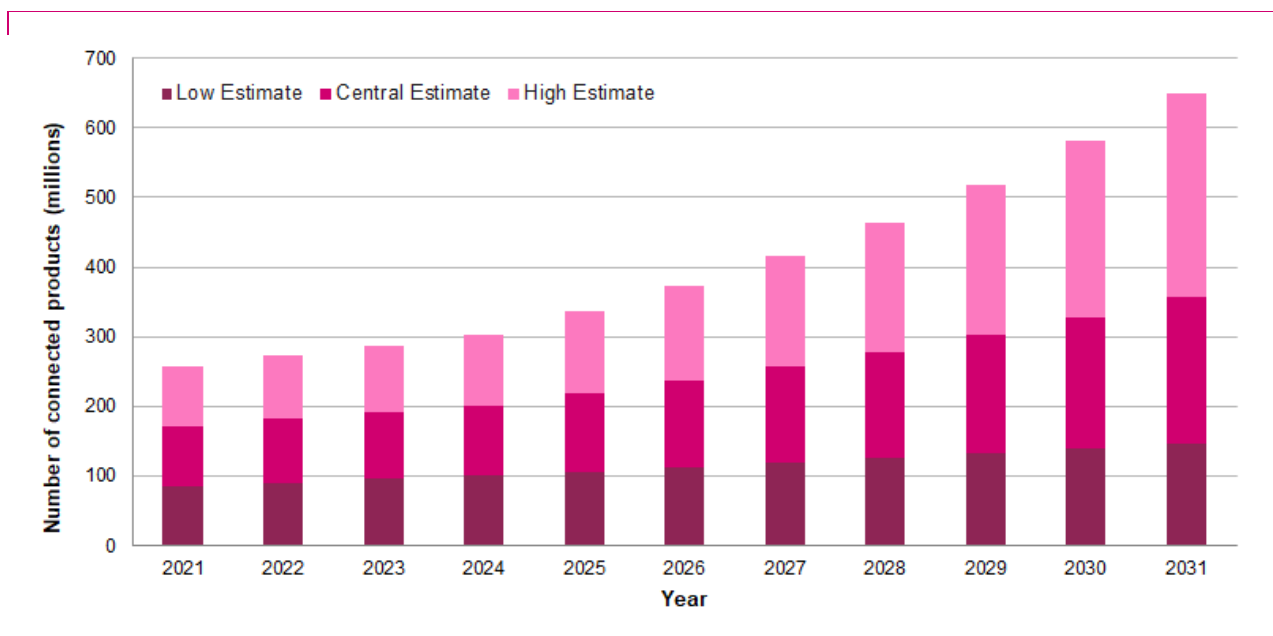
⁹⁰ Strategy Analytics, 2019. Accessed from: <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/>

conventional IT products such as smartphones and tablets with a cellular connection) from 2017 to 2024⁹¹. The five criteria used to define IoT in this research⁹² are that devices must:

- be embedded in everyday objects;
- use an embedded microprocessor;
- connect via the internet;
- use interconnected networks; and
- use standardised communications.

138. This research does not include connectable products that are typically regarded as “conventional IT” such as smartphones, that will be captured within the Government’s intended definition of consumer connectable products. The Ofcom projections have therefore been supplemented with a forecast from Statista ‘of smartphone user numbers in the United Kingdom (UK) from 2018 to 2024⁹³ in order to estimate the total number of consumer connectable products within scope over time.
139. Similarly to the research from Ofcom, the forecast does not cover the entire appraisal period for this policy intervention, which goes until 2031. To this end, in order to forecast the number of connectable products, it was assumed that the number of connectable products within scope grows at a constant growth rate from 2024 onwards (central estimate 11%, worst case estimate 5.5%, optimistic estimate 16.5%). This assumption was based on research from ‘Transforma Insights’, which estimated that between 2020 and 2030, the number of IoT devices worldwide would grow at a compound annual growth rate of 11%.⁹⁴ Sensitivity analysis around the best estimate has been included. In the worst case scenario the growth rate is half that of the central estimate. The optimistic estimate is 50% larger than the central estimate.
140. [Graph 1](#) summarises the projection of the growth of consumer connectable products in the UK (including both “IoT” products and in scope conventional IT products) used for this impact assessment.

Graph 1 - Estimated growth in consumer connectable products in the UK under three scenarios



Estimating the number of new product sold over the appraisal period

141. In order to calculate the estimated benefit of the proposed interventions, it was also necessary to estimate the number of ‘new’ products that would be purchased each year. This is because consumers purchasing ‘new’ products will be affected by the proposed regulation (i.e. products will have a label/built with improved security), while consumers that have purchased an old product (before the policy is implemented) will not be impacted. This is made up of two groups: a) those that buy a new product (additional), and b) those that are buying a product to replace an old one (replacement). Additional products are captured in the estimated

⁹¹ Ofcom, 2017. [Connected Nations Report 2017: Data Analysis](#).

⁹² Cambridge Consultants for Ofcom, 2017. [Review of the latest developments in the Internet of Things](#).

⁹³ <https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/>

⁹⁴ <https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030>

growth of consumer connectable products (see [Graph 1](#)), whereas replacement products are not captured in the growth rate but will still benefit from improved security (depending on the assessed intervention).

142. In order to estimate the impact of intervention, the number of 'new' products purchased each year was estimated using the growth in the total base of products from the previous year (the annual difference between the total number of products, plus an estimate of the number of products that would be upgraded that year (products that are already owned and will be replaced with a new version which, depending on the assessed intervention, may have better security)).
143. In addition to this, it was important to take into account the replacement rate of different products. This is important because the lifespan of products varies and this affects when and how frequently they are replaced.

Estimating the connection rate of consumer connectable products

144. In estimating the impact of intervention, it was important to take into account the connection rate of consumer connectable products, as it is these devices (connected to the internet) that are at risk of a cyber attack.
145. According to the RSM survey commissioned by DCMS, consumers reported that on average, 4% of devices were used, but not connected to the internet, while 3% were owned but not used.⁹⁵ Therefore, the analysis in this impact assessment has assumed that throughout the appraisal period under all scenarios, 92% (rounded to one decimal place) of consumer IoT devices are connected to the internet and are therefore at risk of attack.

7B(ii) - Estimating the replacement rate of consumer connectable products

146. The average replacement rate was estimated for different product categories using data from a consumer survey conducted by YouGov for RSM and other available literature.
147. The 'IoT' product grouping used for the purpose of the RSM survey commissioned by DCMS are set out in [Box 12](#).

Box 12 - IoT product groupings used in "Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT"

Big ticket items - Smart TVs, smart white goods, smart kitchen appliances

Connecting the home - Smart thermostats, home assistants, smart speakers, smart security cameras, smart doorbells

Consumer lifestyle - Smart tablets, smartphones, smart toys, smart watches

148. Estimating the average number of 'replacement' products purchased each year required estimates of the following variables:
 - [The proportion of overall products from each product group](#)
 - [The average life of products in each product group before they are replaced](#)
 - [The distribution across time of when products already owned in each product group were purchased \(i.e. the age profile of existing products\)](#)

Estimating the proportion of overall products from each product group

149. Respondents to a representative consumer survey conducted on behalf of DCMS, reported ownership of consumer connectable products within three high level product groups as follows:⁹⁶
 - **Big Ticket Items:** 56% of people own at least one device in this group
 - **Connecting the Home Items:** 38% of respondents owned at least one device in this group
 - **Consumer Lifestyle:** 92% of respondents owned at least one device in this group
150. The consumer connectable products types included in the product groupings used in the RSM survey (outlined in [Box 12](#)) differed in a number of notable ways across the three product categories. Big ticket items are on average more expensive, which also means consumers tend to own fewer of these products (1.59⁹⁷)

⁹⁵ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

⁹⁶ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

⁹⁷ 1.59 devices owned by households (based on a sample of consumers that reported owning at least 1 device).

compared to connecting the home (2.94⁹⁸). Additionally, the average life of these products differs across the three product categories.

151. The average life cycle of a product affects our methodology for calculating benefits directly as it determines how frequently devices are replaced. The average value of products within each category also impacts the cost to business estimation - as it directly affects the value of the stock disposed of (see [7E\(iv\) - Estimating the costs associated with the disposal of non-compliant goods](#)). Therefore, it was important to estimate the proportion of overall connectable products that fall into each category.
152. The average number of products owned within each category was estimated by multiplying the proportion of people that reported owning a product within each category by the average number of products owned within each category⁹⁹ (see the fourth column of [Table 4](#)). This was then used to determine the proportion of connectable products that fall into each category. These proportions have been used to estimate the number of products within each category - it has been assumed that these proportions remain constant throughout the appraisal period (see the calculated proportions in the fifth column of [Table 4](#)).

Table 4 - Proportion of all products owned in each product category

	% people reporting ownership	Mean number owned if own at least one product	Weighted mean number of products owned	% products owned in each category
Big Ticket Items	56%	1.59	0.89	23%
Connecting the Home	38%	2.94	1.12	29%
Consumer Lifestyle	92%	2.01	1.85	48%
Total	-	-	3.86	100%

Estimating the average life of products in each product group before they are replaced

153. The average life of products within each category also affects the benefits of each intervention because it impacts the frequency with which devices are replaced. The average life of products was estimated using YouGov survey data, and this was used to estimate a group average for each category¹⁰⁰. In estimating the average life of each product category, the popularity of individual products was taken into account (items were assigned a weight dependent on their popularity)¹⁰¹. [Table 5](#) details the average life of each product category estimated using this methodology.

Table 5- Proportion of all products owned in each product category

	Average replacement cycle (years)		
	Central estimate	Worst case	Optimistic case ¹⁰²
Big Ticket Items	9	15	2
Connecting the Home	8	10	2

⁹⁸ 2.94 devices owned by households (based on a sample of consumers that reported owning at least 1 device)

⁹⁹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁰⁰ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁰¹ A more popular item will make up a greater proportion of the total number of devices within a product group. For instance, if smart TV's make up 58% of devices purchased within the 'Big Ticket Item' category it will be assigned a weight of 0.58.

¹⁰² This assumption is based on a Which? Report that suggests security updates for smart appliances end after just 2 years - <https://www.which.co.uk/news/2020/06/the-truth-behind-smart-appliance-security-updates/>

Consumer Lifestyle	4	5	2
---------------------------	---	---	---

154. To forecast the number of devices being replaced on an annual basis, the estimated proportion of devices owned in each category was applied to the forecasted number of UK consumer connectable products.

Estimating the distribution across time of when products already owned in each product group were purchased (i.e. the age profile of existing products)

155. The age profile of UK consumer connectable products as of 2020 was estimated using data from the 2020 RSM consumer survey which, amongst other things, asked consumers about how long they had owned different product types for. Further details of the survey question and presented options are provided in [Table 6](#).

Table 6 - Overview of data from “Evidencing the cost of the UK Government’s proposed regulatory interventions for consumer IoT” used to estimate the age profile of consumer connectable products

Q9 - How long have you had your devices in your household for? Please think about the first one of each type of device you may have had, rather than the existing device”¹⁰³

	Before 2015	Since 2015	Since 2016	Since 2017	Since 2018	Since 2019	Since 2020	Don't know
Big Ticket Items	19%	11%	12%	15%	17%	15%	3%	9%
Connecting the Home	3%	3%	7%	14%	29%	34%	4%	5%
Consumer Lifestyle	10%	5%	9%	13%	24%	26%	3%	9%

156. Whilst the 2020 RSM survey provides data on the exact year of purchase between 2015-2019 it does not for years before 2015. As a result, assumptions were made as to when products were likely purchased¹⁰⁴.
- For example, the average life expectancy of a ‘Big Ticket Item’ is 9 years, which means a ‘Big Ticket Item’ replaced in 2020 (the base year) would have been purchased in 2011 but the consumer survey will only highlight that this item was purchased ‘before 2015’. In the absence of this data, it has been assumed that the proportion of respondents who purchased a ‘Big ticket Item before 2015’ was evenly distributed across the possible years in which it could have been purchased 2011-2014 (is the central estimate).
 - On the other hand, the average replacement rate for ‘Consumer Lifestyle’ products is much shorter (4 years) and therefore these products may have been both purchased and replaced before 2020. To account for this, it was assumed that on average, a quarter of all respondents replaced their ‘consumer lifestyle’ product in the years 2015-2019. This was to ensure that by 2020 these early adopters were included in the replacement cycle.
157. [Table 7](#) details the estimate of the number ‘new’ consumer connectable products (including growth in the total base of products, as well as products that have been replaced) calculated as per the methodology outlined in [7B\(i\) - Estimating the number of consumer connectable products](#) and [7B\(ii\) - Estimating the replacement rate of consumer connectable products](#).

¹⁰³ RSM, 2020. [Evidencing the cost of the UK Government’s proposed regulatory interventions for consumer IoT](#).

¹⁰⁴ See the assumptions log in [Annex 3 - Risks and Assumptions](#).

Table 7 - Total number of 'new' consumer connectable products under the central estimate (in millions)

	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
Replaced	20.6	26.5	10.8	14.3	22.5	27.1	14.9	20.6	28.1	34.6
Growth	4.9	5.0	5.2	11.1	12.3	13.7	15.2	16.9	18.7	20.8
Total New	25.8	31.5	16.0	25.4	34.9	40.8	30.1	37.5	46.9	55.4

7B(iii) - Estimating the cost of cyber attacks

158. The methodology for estimating cyber crime incidents resulting from insecure connectable products involves the following:
- [estimating the frequency of a successful attack occurring](#) (presented as the probability of a consumer of a connectable product falling victim to an attack);
 - [estimating the likelihood of a cyber crime having a financial impact](#); and
 - [data on the average unit cost of an attack](#).

Estimating the frequency of a successful attack occurring**Table 8** - Data on fraud and computer misuse incidents in England and Wales classified as cyber crime

	<i>Fraud</i>			<i>Computer misuse incidents</i>			<i>Overall</i>
	<i>Total incidents</i>	<i>% Cyber Crime</i>	<i>Total cyber incidents</i>	<i>Total incidents</i>	<i>% Cyber Crime</i>	<i>Total cyber incidents</i>	<i>Total cyber incidents</i>
Mar 2019	3,809,000	54%	2,056,860	966,000	97% ¹⁰⁵	937,020	2,993,880
Mar 2018	3,255,000	54%	1,757,700	1,227,000	97%	1,190,190	2,947,890
Mar 2017	3,395,000	56%	1,901,200	1,764,000	97%	1,711,080	3,612,280

Source: Crime Survey for England and Wales, Appendix tables year ending March 2019: A1, Additional tables on fraud and cyber crime year ending March 2018: E6, Experimental tables year ending March 2017: E8; Nature of Crime: fraud and computer misuse data

159. The frequency of a successful attack occurring was estimated using data on (i) the number of fraud and computer misuse incidents classified as cyber crime (see [Table 8](#)) from the Crime Survey for England and Wales and (ii) data on the number of consumer connectable products in the UK¹⁰⁶.
160. A proxy for the frequency or likelihood of a connectable product falling victim to a cyber attack within the UK was estimated by dividing the total number of cyber crime incidents reported in England and Wales by the estimated number of consumer connectable products within England and Wales, which is estimated at 4.4%¹⁰⁷(8.8% in the optimistic estimate and 4.4% in the worst case scenario).
161. As set out in the [NCSC statement 3](#), the 4.4% estimate is likely a 'low estimate' and therefore remains at 4.4% in the worst case scenario but increases to 8.8% in the optimistic scenario (the central estimate has

¹⁰⁵ Note that the proportion of computer misuse incidents identified as cyber crime was not available for the year ending March 2019, therefore it has been assumed that this will remain constant at 97%.

¹⁰⁶ See 'Number of consumer connectable products in the UK' section for estimates (section 7B(i)).

¹⁰⁷ An assumption has been made that the number of consumer connectable products in England and Wales account for 89% of consumer connectable products, which is based on the proportion of the UK population in England and Wales in 2019.

been doubled). DCMS recognises that this is only a proxy and does not reflect the true likelihood of a successful attack resulting from consumer connectable products. This proxy has been used in the absence of data on (i) the true number of cyber crime incidents and (ii) data on the proportion of cyber crime incidents reported that result directly from vulnerabilities and inadequate cyber security measures in consumer connectable products.

- The department has engaged with the NCSC to ensure the selection of a reasonable proxy for this variable (see [NCSC Statement 3](#) for further details).

NCSC Statement 3

Estimating the likelihood of a consumer connectable product falling victim to a cyber attack

“The estimate used here by DCMS is a reasonable proxy given the availability of data. The NCSC advises that this may be a low estimate. In some successful cyber attacks, the owner of the device that is compromised may not necessarily know that the device has been attacked and therefore not report the crime, thus distorting figures. This can be the case in situations such as where a cyber criminal has access to a connected camera in a home for months or years, or where they use a device within a victim’s home to attack other devices in the world.”

Estimating the likelihood of a cyber crime having a financial impact

162. The likelihood of a cyber crime having a financial impact has been estimated using data from the Crime Survey for England and Wales on the proportion of cyber fraud and computer misuse incidents that were recorded by respondents as having ‘an impact’¹⁰⁸. According to this data, 55% of attacks had ‘an impact’ - this has been used as a proxy for the proportion of cyber attacks with a financial impact.
163. DCMS has engaged with the NCSC to assess the appropriateness of using data from the Crime Survey for England and Wales to estimate the likelihood of a cyber crime having a financial impact. [NCSC Statement 5](#) notes that these statistics represent the “best available data to compile an estimate”.

Average unit cost of an attack

164. Lastly, the cost of cyber crime was monetised using data from the Home Office. Research undertaken by the Home Office estimated that the cost to an individual as a result of experiencing cyber crime was £550 per incident, leading to an estimated annual cost of cyber crime of £1.1 billion (based on prices and crime in 2015/16).¹⁰⁹ However, this estimate includes the ‘anticipation of crime’ which is not expected to be affected by any of the policy options being proposed. Therefore, under every policy option (with the exception of the ‘do nothing’ option) the unit cost of cyber crime is assumed to be £281.55 (in 2019 prices) which accounts only for the ‘Economics and social costs of crime research’.¹¹⁰
165. It should be noted that although the anticipation costs are not included in the impact assessment, it is possible that through better cyber security, the anticipation of cyber crime may decrease.

Estimating the cost of cyber attacks resulting from insecure consumer connectable products

166. To estimate the overall total cost to the individual of cyber crime resulting from insecure consumer connectable products, the number of ‘new’ products each year has been multiplied by the probability of attack and the probability of an ‘impact’ occurring.
167. In the ‘do nothing’ option, the direct cost to consumers of consumer connectable product cyber crime has been estimated using the same approach outlined above, however, some methodological differences have been applied.
 - For instance, the whole unit cost of a cyber attack to a consumer of a connectable product has been used. As outlined above, this includes the ‘anticipation of crime’¹¹¹ and amounts to £550 (in 2015/16) prices. The ‘anticipation of crime’ has not been included in other scenarios as it is not expected that the policy options considered will affect this - consumers will likely still anticipate cyber crime, with or without the proposed interventions. To this end, DCMS have taken a conservative approach to estimating the unit cost of a cyber attack.
 - The majority of assumptions underpinning the methodology remain the same. The proportion of consumers of connectable products relative to the proportion of businesses is identical across options. An assessment of the ‘businesses as consumers’ of consumer connectable products can be found in the subsequent section [7C - Benefits methodology of relevance to all options](#).
168. The overall direct cost (cyber attacks resulting from inadequate security provisions in consumer connectable products) to consumers and businesses under the ‘do nothing’ option across the 10 year appraisal period, and a summary of the methodology for calculating this figure, is presented in [Table 9](#).

¹⁰⁸ Crime Survey for England and Wales, Appendix tables year ending March 2019 - <https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingmarch2019>

¹⁰⁹ Heeks M., Reed S., Tafsiri M., Prince S., 2018. [The economic and social costs of crime Second edition](#)

¹¹⁰ Heeks M., Reed S., Tafsiri M., Prince S., 2018. [The economic and social costs of crime Second edition](#)

¹¹¹ Heeks M., Reed S., Tafsiri M., Prince S., 2018. [The economic and social costs of crime Second edition](#)

Table 9 - Overall direct cost (cyber attacks resulting from inadequate consumer connectable product security) to consumer and businesses across the appraisal period under the 'do nothing' option

	Total products		Proportion Owned		Probability of attack		Probability of impact		Unit cost of an attack		Overall cost
	A	x	B	x	C	x	D	x	E	=	ABCDE
Consumers	1.35bn	x	82%	x	4.4	x	55%	x	£282	=	£14.8bn
Businesses		x	18%	x		x	46%	x	£990	=	£4.8bn
											Total
											£19.6bn

Key:

- A = Estimated number of consumer connectable products over the appraisal period connected to the internet
- B = Proportion of consumer connectable products owned by consumers / businesses
- C = Probability of a cyber attack
- D = Probability that a cyber attack has a financial impact on a consumer / business
- E = Average unit cost of an attack to consumers / businesses (2019 prices)

7C - Benefits methodology of relevance to all options

7C(i) - Estimating the benefits resulting from reduced cyber crime

169. In all scenarios (short-listed policy options), consumers benefit from more secure connectable products. Consumers benefit because improved security means they are less likely to become a victim of a cyber attack. Therefore, in all scenarios, the benefits have been monetised by estimating the reduction in the number of cyber crime incidents (relative to the status quo/do-nothing option), and multiplying this reduction by the unit cost of an attack.

Estimating the impact of baseline security measures on the likelihood of cyber crime

170. Fundamental technical barriers preclude the gathering of evidence that would enable the reduction in cyber crime incidents resulting from enhanced security measures to be quantified (see [NCSC Statement 4](#) for further details). The reduction in the number of cyber crime incidents has therefore been estimated by multiplying the number of 'new' products with improved security (as a result of intervention) by the reduction in the probability that they become victims of an attack (50% reduction central estimate, 20% worst case estimate and 80% optimistic estimate)¹¹². This was then multiplied by the probability that an attack has an impact.
171. The department has engaged with the NCSC to ensure the selection of a reasonable methodology for estimating the reduction in the probability of a cyber attack following the implementation of baseline security measures (see [NCSC Statement 4](#) for further details).

¹¹² In the absence of data linking crime specific to consumer connectable products these estimates have been judged by NCSC as reasonable (see [NCSC Statement 4](#)).

NCSC Statement 4

Estimating the reduction in the probability of a cyber attack following the implementation of baseline cyber security measures

“The NCSC note that there is no quantifiable evidence to be able to gauge or analyse crime specific to connected consumer devices for the following reasons:

- *Many attacks against connected consumer devices are invisible to the user, and so will not be reported.*
- *It is difficult to determine what is, and isn't an attack. For example, the communications to a connected consumer device of someone legitimately logging in using universal default credentials, would look effectively identical to a malicious user attempting to log in using those same credentials. Conversely, a botnet enabled DDoS attack on a small scale, may not have an impact on an internet facing service, but would still likely be classified as an attack.*

Producing an estimate for the reduction in probability of a successful cyber attack is therefore inherently challenging. New techniques could be employed by attackers to exploit vulnerable devices and it's difficult to predict what security mitigations industry could employ to protect consumer devices. Given the lack of evidence and based on NCSC's view that these requirements will reduce the threat of cyber attacks to consumers (see [NCSC Statement 1](#)), DCMS's estimates highlighted above are reasonable”.

Estimating existing compliance levels with the minimum security baseline

172. In order to estimate the number of 'new' products with improved security it was necessary to estimate the proportion of consumer connectable products that currently meet the minimum security baseline (three security requirements aligned to the top three guidelines of the Code of Practice, see [Section 5 - Description of shortlisted interventions, preferred option, and plan for implementation](#) for further details). Owners of products that are already compliant with the initial baseline security measures the shortlisted options are seeking to mandate or encourage the uptake of will not directly benefit from a reduced likelihood of falling victim to a cyber attack.
173. The current compliance rate has been estimated by combining data from Which? Investigations and the Which? consumer test programme with research conducted by the Internet of Things Security Foundation. We estimate that only 0.27% of consumer connectable products met all three security requirements in the initial minimum security baseline¹¹³. This has been used as a proxy for the current level of compliance. Furthermore, the benefits have been calculated under the assumption that consumers will benefit from improved security in instances where all three security requirements aren't met (by products they already own when replacing their product with a new one¹¹⁴).
174. It has also been assumed in all cases that the probability of a successful attack having an impact is constant at 55%. This assumption is based on the proportion of cyber crime that was reported in the Crime Survey for England and Wales as having an impact (see the preceding section - [Estimating the likelihood of a cyber crime having a financial impact](#)). It should also be noted that DCMS has engaged with the NCSC to assess the appropriateness of this estimate (see [NCSC Statement 5](#) for further details).

¹¹³ For the purposes of this impact assessment, Which? submitted data from their investigations and consumer test programme between October 2019 and January 2021 concerning the security of 253 consumer connectable products. The estimate of overall probability of a product complying with all three security requirements has been derived from the probability that a device randomly sampled from the products investigated by Which? met security requirement 1 (no universal default passwords) and security requirement 3 (security update transparency), and that it also met security requirement 2 (having a vulnerability disclosure policy), based on separate estimates of compliance with this requirement outside of the Which? data. Which? Tested for (i) default passwords and (iii) security updates. The proportion of consumer IoT found to have a Vulnerability Disclosure was 18.9% according to the IoTSF report “Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure, which has been used to estimate current compliance with this security requirement. This estimate of compliance with security requirement 2 was used in combination with the Which? data to estimate the proportion of products compliant with the minimum security baseline.

¹¹⁴ Note that we have assumed consumers will benefit from the proposed regulation if they currently own a product that is non-compliant. A non-compliant product has been defined as one that does not meet all three security requirements. We have also assumed that the level of protection consumers receive from switching to a non-compliant product to a compliant product is the same in every case. In reality, this will depend on how secure the consumer's current product is (i.e does it currently meet two of the proposed security requirements or none).

NCSC Statement 5 - Use of statistics from the Crime Survey for England and Wales

“Further to the points raised in [NCSC Statement 4](#), NCSC agrees with DCMS's decision to use the Home Office's Crime Survey statistics as the best available data to compile an estimate however it is important to note the following assumptions that have to be taken with this data:

- *The detail within the Crime Survey data does not allow a determination over whether a security issue with a connected consumer device enabled that particular attack.*
- *The Crime Survey data does not include the impact of invisible attacks, where the user is not aware that it has happened or been successful. This causes a skew in the Home Office crime survey that will undercount the total number of cyber attacks”.*

Additional benefits methodology considerations

175. Benefits are assumed to be cumulative under all policy options, taking into account the length of time that different categories of device are estimated to be used in each scenario. This is because a more secure product, once purchased, will continue to provide security benefits to the owner for as long as the product is in use. Therefore, the longer that the policy is in place, the larger the benefits will be, as an increasing number of devices owned by UK consumers will have a basic level of security.
176. It should also be considered that the model used for this indicative cost-benefit analysis only takes into account the direct benefit of costs avoided by the individual and the indirect benefit to businesses who use consumer connectable products. The benefits to wider society increase exponentially as the more products with appropriate minimum security measures are adopted. This is because the more products that meet the minimum security baseline, the smaller the attack surface for malicious actors to take advantage of.

Estimating the benefits to business of improving consumer connectable product security

177. Connectable products primarily intended to be employed in industrial applications are not in scope of this policy. However, the department recognises that (i) businesses are also consumers of consumer connectable products and (ii) the impact to business from a cyber attack differs from the impact felt by a consumer. Therefore, to accurately estimate the benefits from the proposed policy option it is essential to estimate the proportion of consumer connectable products owned by businesses and the average cost of a cyber attack to a business as opposed to a consumer.
178. In all scenarios (policy options), an estimate has been made around the proportion of consumer connectable products used by businesses relative to the proportion used by consumers¹¹⁵. This distinction has been made primarily due to the difference in potential costs faced by businesses as opposed to consumers with regard to a cyber attack. The best estimate is that 18% of consumer connectable products are owned by businesses - this estimate is based on the proportion of network connected products within the ‘business segment’¹¹⁶ multiplied by the estimated proportion of connected products used by businesses that fall within the scope of the proposed regulation¹¹⁷. Sensitivity analysis has been used around this assumption (9% in the worst case scenario and 26% in the optimistic scenario). For the sensitivity analysis, the central estimate has been increased and decreased by 50%.
179. The approach to estimating the benefits to businesses as users of consumer connectable products, for all scenarios, is the same as the approach to estimating the benefits for consumers of connectable products, with the exception of the following differences to underlying assumptions:
 - Data from the Cyber Security Breaches Survey 2020 has been used to estimate the cost to business from a successful cyber attack. This is estimated to cost businesses £1,010 per incident - this differs to the average cost per attack to an individual.
 - The probability of a successful attack has been assumed to be slightly lower for businesses (46%)¹¹⁸. This is based on data from the Cyber Security Breaches Survey.

¹¹⁵ In line with RPC Guidance, these benefits to businesses have not been factored into the EANDCB calculation as they are considered an indirect impact.

¹¹⁶ <https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/air-highlights.html#>

¹¹⁷ The data on page 4 of the following analysis of enterprise IoT traffic has been used to estimate the proportion of devices that are likely to be in scope. It suggests that 67% of IoT devices on enterprise networks could be considered consumer connectable products, and would therefore fall in scope of this policy initiative: https://www.zscaler.com/resources/industry-reports/iot-in-the-enterprise.pdf?_ga=2.167275966.1267039324.1582731852-1521726222.1582731852

¹¹⁸ Cyber Security Breaches Survey 2020 - <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020>

- It is also worth mentioning that businesses are considered to benefit indirectly from the proposed regulation as opposed to household consumers who directly benefit from improved security.

Estimated benefits of Option A - Voluntary security labelling scheme

180. The benefits of a voluntary label are assessed to be the reduction in risk of cyber attacks as a result of more consumers buying connected products that meet the top three Code of Practice cyber security guidelines. A conservative approach has been used to quantify benefits, assuming that benefits will be realised from year two of the appraisal period, as manufacturers start to adopt the label from year one onwards.
181. In both labelling scheme scenarios, unlike policy option C, non-compliant devices can still be purchased, which means the benefits in these scenarios depend on (i) consumer behaviour (i.e the proportion of consumers that are incentivised to switch to more secure products) as well as business behavior (the extent to which businesses sell compliant products/with a positive label). Therefore, in order to estimate the benefits it was necessary to make further assumptions. Firstly, an assumption was made on the proportion of products produced with a positive label and secondly an assumption was made on the proportion of consumers that change behaviour (proportion of consumers that switch to products with a positive label as a result of the label and the information it contains)
182. The benefits methodology under the labelling scheme options, like the mandatory security baseline option (Option C), depend on estimating the avoided cost of cyber crime (see the preceding section - [7C\(i\) - Estimating the benefits resulting from reduced cyber crime](#) for details). This methodology rests on calculating the number of consumer connectable products purchased with improved security requirements (as a result of intervention). In this case, this depends on the number of 'new' consumer connectable products sold with a 'positive label' (i.e products that meet the minimum security baseline) and the likelihood of a label incentivising consumers to purchase a device with a positive label. This has been estimated by multiplying the proportion of 'new' consumer connectable products with a positive label by the probability that a consumer is incentivised to switch/purchase a more secure product as a result.
183. Under the central scenario, it has been assumed that in year 2, 1.8%¹¹⁹ of new products are purchased with a positive voluntary label and that this remains constant throughout the appraisal period. We expect consumer awareness of the labelling scheme to improve over time, and we expect that this will translate into a higher proportion of consumers adopting a product with a 'positive label'. To reflect this, we have increased the probability that a consumer is incentivised to purchase a product with a 'positive label' over the appraisal period. It has been assumed that 10% of consumers are incentivised to purchase a product with a positive label in year 2 (i.e are influenced by the label) but that this increases by 1% per year throughout the appraisal period to 19% in year 10¹²⁰. This is based on evidence from food labelling research, which suggests that between 10-25% of consumers made healthier choices as a result of different types of food labels (see [Table 38](#)). The estimates above are more conservative (i.e start at 10% in year 2) because we assume that consumer awareness and knowledge of cyber security is likely to be lower than that of healthy food choices, the proportion of consumers who purchase a product with a positive security label will increase over time as awareness increases. Therefore, in this scenario in 2023 there is a 0.18% chance that a consumer switches to a product with a positive label (1.8%*10%).
184. In the worst case scenario, it has been assumed that only 0.27% of new products are purchased with a positive label throughout the appraisal period and that similarly to the central scenario, 10% of consumers are incentivised to switch to a product with a positive label and this increases year on year. Research by Harris Interactive found that 51% consumers said that they would consider switching from their usual brand of smart devices to one that had a label.¹²¹ Therefore, in the optimistic scenario, it has been assumed that 1.8% of 'new' products purchased would have a positive label and that 51% of consumers are incentivised to purchase a product with a 'positive label' (a 0.9% chance that a consumer switches to a product with a positive label).

¹¹⁹ This is based on the number of businesses (3) that have publicly committed their adoption of the security requirements set out in the code of practise, as a proportion of UK manufacturers (170).

¹²⁰ The following process has been taken to estimate the number of new products sold to consumers as a result of intervention: First, the annual number of 'new' consumer connectable products has been estimated (replacement rate plus growth in base of consumer connectable products, by product category). Second, these estimates are multiplied by step 3 in [Table 11](#) in order to estimate the annual number of new products sold to consumers as a result of intervention. Third, taking into account the length of time that different categories of product are in use, the annual number of new products (sold to consumers as a result of intervention) still in use has been estimated (i.e benefits are cumulative). Lastly, the estimates from step three have been multiplied by the probability that a device is connected to the internet (92%). The estimates from this process can be found in [Table 10](#).

¹²¹ Harris Interactive -

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

Table 10 - Estimated increase in the number of new products sold to consumers with improved security, still in use, in thousands (*Policy option A - Voluntary Security Labelling Scheme*)

	2023	2024	2025	2026	2027	2028	2029	2030	2031
Worst Case	6	13	18	23	31	36	39	46	55
Central Estimate	52	81	132	207	256	314	386	479	590
Optimistic Case	405	831	946	1,105	1,244	1,400	1,577	1,776	2,003

Table 11 - Total estimated benefits (*Policy option A - Voluntary Security Labelling Scheme*)

#	Step	Worst Case	Central Estimate	Optimistic Case
1	Proportion of products with a 'positive label'	0.27%	1.8%	1.8%
2	Proportion of consumers influenced by the 'positive label'	10% in 2023, rising by 1% a year	10% in 2023, rising by 1% a year	51%
3 (1*2)	Probability that a consumer is incentivised to purchase a product with a 'positive label'	0.03% in year 2	0.18% in year 2	0.9%
4	Estimated increase in the number of products sold to consumers with increased security	Probability that a consumer is incentivised to purchase a product with a 'positive label' * number of 'new consumer connectable products' See Table 10		
5	Impact of improved security	See section: 7C(i) - Estimating the benefits resulting from reduced cyber crime		
6 (4*5)	Estimated number of attacks avoided	Estimated increase in the number of products sold to consumers with increased security * Impact of improved security		
7	Average unit cost of an attack ¹²²	£352	£406	£468
8	Benefits	Estimated number of attacks avoided * Average unit cost of an attack		
Total estimated benefits		£1.8m	£35.9m	£186.2m

Estimated benefits of Option B - Mandatory security labelling scheme

185. The benefits of a mandatory labelling scheme are estimated to be greater than that of a voluntary labelling scheme, as all products will be required to provide information about security features, which will help to inform consumers' purchasing decisions.

¹²² The average weighted unit cost of an attack across businesses and individual consumers. The difference in cost is driven by the difference in business to individual consumer ratio across scenarios (i.e in the central estimate businesses make up 18% of consumers but 26% in the optimistic scenario).

186. The benefits arising from the mandatory labelling scheme have been estimated in a similar way to the 'voluntary labelling scheme'. Similarly to the voluntary scheme, assumptions have been made around (i) consumer behaviour and (ii) business behaviour (the extent to which businesses sell compliant products/with a positive label).
187. Under the mandatory labelling scheme as well as the voluntary scheme, it is assumed that security of connectable products will improve as the label incentivises manufacturers to adopt higher levels of security. However, there is a risk that leading up to the regulations coming into force, retailers may sell non-compliant products or products that would otherwise have a negative label at a reduced price, leading to an increase in the number of insecure products being purchased without the consumer being aware. This may also reduce the benefits in the short term.
188. It will also take time for consumers to adjust their purchasing habits and be encouraged to choose devices with a positive label. To reflect this, it has been assumed that (i) the proportion of consumers that change behaviour (incentivised to purchase a product with a positive label) grows gradually over the appraisal period and therefore (ii) the proportion of products with a positive label also grows gradually over the appraisal period (as better consumer awareness incentivises more businesses to adopt security measures aligned to the minimum security baseline).
189. Under the central scenario, it has been assumed that in year 2, 25% of new products are purchased with a positive label and that this rises to 90% in 2026 and remains at 90% through to the end of the appraisal period¹²³. This essentially means we expect, at least in the short run, that the majority of consumer connectable products will continue to be sold without the proposed security requirements. That said, we expect it to be significantly higher than the 'do nothing' scenario in which there is little incentive for manufacturers to adopt these security measures (current compliance is estimated to be 0.27%). The reason we expect this to rise over time (increase to 90% by 2026) is we expect the mandatory label to improve consumers' awareness and understanding of the level of security built into their device. Moreover, as consumer awareness increases, we expect there will be more pressure on manufacturers to adopt better security practises (i.e adopt the suggested security requirements). However, the extent and rate at which the mandatory labelling scheme incentivises manufacturers to adopt better practises is highly uncertain. Therefore, sensitivity analysis has been used.
190. Similarly to the voluntary labelling scheme, it has been assumed that 10% of consumers are incentivised to purchase a product with a positive label in 2023 but that this increases by 1% per year throughout the appraisal period to 19% in year 10.
191. In the worst case scenario, it has been assumed that only 13% of new products are purchased with a positive label throughout the appraisal period and that 10% of consumers are incentivised to purchase a product with a positive label in 2023 but that this increases by 1% per year throughout the appraisal period to 19% in year 10.
192. In the optimistic scenario it has been assumed that 50% of 'new' products purchased have a positive label in year 2 and that this rises gradually to 90% in year 4 of the appraisal period¹²⁴. In the optimistic scenario it has been assumed that 51% of consumers are incentivised to purchase a product with a 'positive label'.

¹²³ Assumption is 25% in 2023; 50% in 2024; 75% in 2025 and 90% from 2026.

¹²⁴ Assumption is 50% in 2023; 75% from 2024 and 90% from 2025.

Table 12 - Estimated increase in the number of new products sold to consumers with improved security, still in use, in thousands (Policy option B - Mandatory Security Labelling Scheme)

	2023	2024	2025	2026	2027	2028	2029	2030	2031
Worst Case	360	772	1,001	1,294	1,723	2,007	2,151	2,513	3,003
Central Estimate	724	1,534	3,640	7,392	11,494	14,751	18,580	23,221	28,910
Optimistic Case	11,239	29,002	43,770	55,260	62,177	69,992	78,828	88,823	100,137

Table 13- Total estimated benefits (Policy option B - Mandatory Security Labelling Scheme)

#	Step	Worst Case	Central Estimate	Optimistic Case
1	Proportion of products with a 'positive label'	13%	25% in year 2 rising gradually to 90% by 2026	50% from year 2 rising to 90% from year 4
2	Proportion of consumers influenced by the 'positive label'	10% in 2023, rising by 1% a year	10% in 2023, rising by 1% a year	51%
3 (1*2)	Probability that a consumer is incentivised to purchase a product with a 'positive label'	1.3% in year 2	2.5% in year 2	26% in year 2, rising to 46% from year 4
4	Estimated increase in the number of products sold to consumers with increased security ¹²⁵	Probability that a consumer switches to a product with a 'positive label' * number of 'new consumer connectable products' See Table 12		
5	Impact of improved security	See section: 7C(i) - Estimating the benefits resulting from reduced cyber crime		
6 (4*5)	Estimated number of attacks avoided	Estimated increase in the number of products sold to consumers with increased security * Impact of improved security		
7	Average unit cost of an attack ¹²⁶	£352	£406	£468
8	Benefits	Estimated number of attacks avoided * Average unit cost of an attack		

¹²⁵ The following process has been taken to estimate the number of new products sold to consumers as a result of intervention: First, the annual number of 'new' consumer connectable products has been estimated (replacement rate plus growth in base of consumer connectable products, by product category). Second, these estimates are multiplied by step 3 in [Table 13](#) in order to estimate the annual number of new products sold to consumers as a result of intervention. Third, taking into account the length of time that different categories of product are in use, the annual number of new products (sold to consumers as a result of intervention) still in use has been estimated (i.e benefits are cumulative). Lastly, the estimates from step Three have been multiplied by the probability that a product is connected to the internet (92%). The estimates from this process can be found in [Table 12](#).

¹²⁶ The average weighted unit cost of an attack across businesses and individual consumers. The difference in cost is driven by the difference in business to individual consumer ratio across scenarios (i.e in the central estimate businesses make up 18% of consumers but 26% in the optimistic scenario).

Estimated benefits of Option C - Mandatory security baseline

193. The benefits that arise from policy option C are realised as “new” consumer connectable products are purchased that comply with the mandatory security baseline. The same replacement rate scenarios have been used across all options, however, under option C, all devices purchased after year 2 would have to comply with the minimum security baseline. Therefore, the proportion of consumers that currently don’t own a compliant product but purchase a device from year 2 will benefit from the reduced risk of falling victim to a cyber attack.
194. Benefits accumulate over time as more products are owned which comply with the security baseline, taking into account the average life of products (based on the estimated length of time products are used by consumers in each category). Therefore, each year after the legislation has been implemented (year 2 onwards), the number of ‘new’ products has been calculated as the products purchased that year plus products purchased in previous years that are still in use (taking into account the average expected life of a product in each of the three categories).
195. It is expected that mandating aspects of the top three security guidelines from the Code of Practice would have a greater impact on improving security compared to a mandatory security label. This is because all in-scope products made available on the UK market will meet the initial security baseline, whereas with a security label, insecure products would still be available to be purchased on the market.
196. According to the 10th annual Verizon Data Breach Investigations report (2017), 81% of hacking related breaches involved stolen or weak passwords.¹²⁷ Further, a January 2018 F-Secure IoT Threat Landscape report found that threats targeting weak/default credentials, unpatched vulnerabilities, or both, made up 87% of observed IoT threats.¹²⁸ Therefore, it is anticipated that implementing these basic security controls could have a significant impact in preventing many everyday threats to consumer connectable products.
197. Benefits may also accrue more quickly than if a label were mandated, as it may take time for manufacturers and consumers to change their behaviour in response to providing minimum security information on product packaging. Moreover, this option doesn’t rely on consumers becoming more informed about consumer connectable product security and changing their purchasing patterns toward products that have higher levels of security, as all products will be required to meet the minimum security standard.
198. [Table 15](#) below details the steps taken to estimate the benefits under this scenario. The first step involves estimating the annual number of ‘new’ consumer connectable products that meet the following two conditions; 1) the product must not currently meet the three security requirements¹²⁹ 2) the product must be connected to the internet¹³⁰. If these two conditions are met, the consumer will benefit from the policy proposal for as long as the product is in their possession. [Table 14](#) outlines the estimated number of ‘new’ products in use during the appraisal period that meet the conditions described above.

¹²⁷ 2017 Data Breach Investigations Report, Verizon. - <https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf>

¹²⁸ IoT Threat Landscape: Old hacks, new devices <https://blog-assets.f-secure.com/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf>

¹²⁹ As outlined previously, DCMS estimate that only 0.27% of consumer connectable products on the UK market are compliant with all three security requirements. All non-compliant devices are captured in the benefits calculation.

¹³⁰ DCMS estimates that 92% of all consumer connectable products are connected to the internet. Only devices connected to the internet are at risk of a cyber attack and therefore devices not-connected to the internet are not captured in the benefits.

Table 14 - Total number of 'new' consumer connectable products still in use, in millions
(Policy option C - Mandatory Security Baseline)

	2023	2024	2025	2026	2027	2028	2029	2030	2031
Worst Case	23	47	60	75	95	102	103	115	131
Central Estimate	24	36	55	81	92	107	125	147	171
Optimistic Case	32	66	76	88	99	112	126	142	160

Table 15 - Total estimated benefits (Policy option C - Mandatory Security Baseline)

#	Step	Worst Case	Central Estimate	Optimistic Case
1	Estimated number of 'new' consumer connectable products in use throughout the appraisal period with improved security and connected to the internet	See Table 14	See Table 14	See Table 14
2	Estimating the likelihood of a cyber attack	(Probability of attack)*(Probability of impact)	(Probability of attack)*(Probability of impact)	(Probability of attack)*(Probability of impact)t
3	Impact of improved security	20% reduction in the likelihood of cyber attack	50% reduction in the likelihood of a cyber attack	80% reduction in the likelihood of a cyber attack
4 (2*3)	Estimated fall in the number of cyber incidents	(Estimated number of 'new' consumer connectable products in use throughout the appraisal period with improved security and connected to the internet) *		
		(Likelihood of a cyber attack * Impact of improved security)		
5	Average unit cost of an attack ¹³¹	£352	£406	£468
Total estimated benefits		£1,074.1m	£8,015.2m	£34,172.2m

199. [Table 16](#) presents the total estimated benefits for Policy Option C - Mandatory security baseline alongside the estimated benefits for all other shortlisted policy interventions. It should be noted that the benefits are expected to be the highest under the preferred policy option as it is the only option, in which all new products comply with the minimum security baseline (relative to the our estimate of existing compliance levels, 0.27%).

¹³¹ The average weighted unit cost of an attack across businesses and individual consumers. The difference in cost is driven by the difference in business to individual consumer ratio across scenarios (i.e in the central estimate businesses make up 18% of consumers but 26% in the optimistic scenario).

Table 16 - Total estimated benefits under all shortlisted policy interventions

		Worst Case	Central Estimate	Optimistic Case
A	Voluntary security labelling scheme	£2.0m	£33.9m	£314.1m
B	Mandatory security labelling scheme	£110.3m	£2,017.8m	£10,763.5m
C	Mandatory security baseline	£1,074.1m	£8,015.2m	£34,172.2m

7C(ii) - Non-monetised benefits

200. While the department has attempted to monetise all potential benefits that may result from improved security, it has not been possible to quantify all benefits. All non-monetised benefits are outlined below and apply to all policy options.
201. Firstly, it is possible that the UK's consumer connectable product sector may grow as a result of increased consumer confidence, leading to increased adoption. This could potentially lead to lifestyle benefits, for example higher productivity, finding it easier to connect to the internet, improved efficiency and control within the home which could lead to energy savings¹³².
202. Proportionate measures to improve the baseline cyber security of these products could increase adoption rates amongst previously sceptical consumers. Evidence shows that amongst consumers who said that they didn't plan on purchasing a smart device in the next 12 months, 30% were concerned about their privacy and 28% concerned about the security of devices. Of those that said they were unlikely to purchase a smart device due to security, privacy or quality concerns, 28% said that independent certification / assurance to a minimum standard would encourage them to purchase, followed by transparency on the length of time security updates would be provided (22%), assurance that every device has a unique password (20%), security information at the point of sale and assurance from manufacture of adherence to minimum standard (both 19%).¹³³
203. DCMS has engaged with the NCSC to assess the possibility of accurately monetising the potential benefits to society that may result from a reduction in the number and scale of DDoS attacks (see [NCSC Statement 6](#) for further details). It has not been possible to accurately estimate these costs due to the unpredictability of when these events will occur, in terms of scale, impact and how often they will occur. Previous cyber attacks based on malware, such as from Mirai, Reaper, and Satori, are illustrative of the potential impacts that can occur as a result of botnet attacks using connectable products (see [2D - Botnets, and the impact of insecure consumer connectable products on networks and infrastructure for further details](#))

NCSC Statement 6

Assessing all costs relating to cyber breach attacks

“The NCSC agrees with DCMS that it is not possible to monetise accurately all the potential benefits that may result from a reduction in cyber attacks linked to vulnerabilities in connectable products, such as invasion of privacy, ransomware attacks or DDoS attacks. This is because it is very difficult to assess the full impact of an attack on both the consumer and wider society, including companies and digital infrastructure. The harms resulting from a cyber attack are numerous and not purely financial or reputational. An attack can also cause psychological problems to people affected by attacks and these can be broken down into further sub categories (impact on the user's other devices, their day to day living etc). It is therefore not possible for DCMS to capture all the costs relating to such large scale attacks”.

204. A conservative approach to modelling the benefits has also been taken within this impact assessment because benefits have been assumed to start from year two of the appraisal period for all policy options, while costs to businesses have been incurred from year one. This is a conservative assumption, as it is

¹³² <https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf>

¹³³ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

possible that manufacturers will make changes within the first year. However, as there will likely be a 12 month transition period it is more likely that economic operators use this time to prepare for the legislation.¹³⁴

7D - Costs methodology of relevance to all options

7D(i) - Estimating the number of manufacturers and retailers of consumer connectable products

205. In order to scale the impact of the proposed interventions to the national level, the average cost to manufacturers/retailers is multiplied by the estimated number of organisations in scope.
206. The IoTUK Nation Database provides a list of UK IoT businesses which could be in scope of the PSTI product security measures.¹³⁵ This database, last updated in August 2018, includes 69 IoT manufacturers of computer, electronic and light electrical products, which has been used as the optimistic case estimate for the number of manufacturers in scope. Research conducted by RSM in 2020 found 170 manufacturers that sell their products to the UK market, which has been used as the central and worst case estimate for UK based consumer IoT manufacturers.¹³⁶
207. Manufacturer cost is likely to be an overestimate, as the cost to businesses as defined by impact assessment guidance only considers business activity that occurs in the UK, while many electrical goods are manufactured elsewhere and imported to the UK. There is a lack of data on the proportion of all consumer connectable products sold in the UK that are manufactured in the UK, so a conservative approach has been taken which assumes that all costs incurred as a result of regulatory options on manufacturers fall on UK business activity.
208. Data from Statista has been used to estimate the number of retailers in scope. More specifically, the number of UK retailers within the electrical appliances sector has been used as a proxy for the number of retailers of consumer connectable products. According to this data, there were 3485 retailers in 2020.¹³⁷ This estimate has been used for both the central and optimistic estimate. However, in the worst case scenario it has been estimated that there are 3,675 retailers within scope¹³⁸. Furthermore, although second hand markets are not within scope of the proposed legislation, we have assumed that charities will still spend time familiarising themselves with these proposals. In the optimistic scenario it has been estimated that there are 5,600 charities within scope. In both the worst case and central scenario it has been estimated that there are 11,200 charities within scope - these estimates are based on data from the Charity retail association.¹³⁹

7D(ii) - Estimating familiarisation costs

209. Under all scenarios, both manufacturers and retailers will have to spend time familiarising themselves with the legislation. RSM conducted a survey on behalf of DCMS to collect evidence on the time it would take for organisations to familiarise with different regulatory options, and the job roles that would be involved¹⁴⁰. More specifically, respondents were asked to estimate the number of person-days undertaken by each job role who may be involved in the familiarisation process to understand any new regulation on compliance with aspects of the top three Code of Practice guidelines. The financial cost of this time has been monetised using the wage bands outlined in [Table 17](#) and multiplying this by the estimated amount of time required for each job role. The estimated cost of this time has been averaged across respondents for both (i) manufacturers and (ii) retailers (retailers and charity shops) and then scaled up by multiplying the estimated average cost by the number of retailers in scope (see [7D\(i\) - Estimating the number of manufacturers and retailers of consumer connectable products](#)).

¹³⁴ Following Royal Assent, DCMS are planning to have a 12 month transition period before the legislation comes into force. The enforcing authority may work with economic operators during this period to support them to achieve compliance with the legislation but will not take enforcement action. This will enable economic operators time to prepare for the legislation .

¹³⁵ <https://datamillnorth.org/dataset/iotuk-nation-database>

¹³⁶ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹³⁷ <https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/>

¹³⁸ This estimate includes the 3,485 retailers already identified plus 190 retail chains identified as potentially being within scope. To avoid double counting the number of retail chains within the 'consumer electronics' sector are not included -

<https://www.statista.com/statistics/642131/retail-chains-number-by-sector-uk/>

¹³⁹ <https://www.charityretail.org.uk/charity-shops-faq/> - note that the 11,200 figure represents the number of shops and not the number of organisations. It is therefore an overestimate.

¹⁴⁰ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

Table 17 - Salary Assumptions

Role	Daily Rate	Annual	Job role from national career service
IT or technical director or equivalent	£426	£110,663	Head of IT
IT specialist manager	£205	£53,345	Test Lead IT
IT professional or technical role	£181	£47,103	Robotics engineer
Non-IT professional role (e.g. legal accounting)	£229	£59,588	Company secretary
Administrative	£116	£30,078	Office manager
Sales and Marketing professional	£166	£43,130	Retail merchandiser
Other	£124	£32,284	Average national wage (ONS)

Notes: This table has been taken from the RSM report 'Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT', 2020. The data comes from the National careers average salary data.

Policy Options A and B - Labelling Scheme Options

210. Both manufacturers and retailers would have to spend time familiarising with the legislation and the implications for their businesses. For the product labelling option, manufacturers estimated that 11.8 person days would be required on average for familiarisation. In terms of the labelling scheme, respondents felt it would mostly be the responsibility of professional roles in IT and other areas such as legal or accounting. The overall estimate of this one-off cost is just £1,585. However, to account for the small sample size (only 4 manufacturers responded) sensitivity analysis has been used (the optimistic estimate has been reduced by 20% in the worst case scenario and increased by 20%).
211. In total, 1886 retailers were directly asked to take part in the RSM survey, however, the survey only received 12 valid responses. Therefore, due to the low response rate, these results are indicative and should be interpreted with caution.
212. Retailers, like manufacturers, were asked to estimate the one-off familiarisation costs, in terms of staff time, to read and understand proposed legislation if an IoT security label that indicates whether products adhere to the three guidelines of the Code of Practice were introduced. All but one said that there would be costs in person days from administrative, sales advisor or customer services representative level, through to corporate manager and director level. However, in this case, the maximum estimated costs to organisations to read and understand the proposed legislation would be one to two person weeks, and that would be for managers or those in commercial and procurement roles, while for administrative, sales advisor and customer services representative roles there would only be a maximum cost of two to three person days¹⁴¹. This, on average, amounted to a cost of £1,676 for retailers. An assumption has been that charity shops will face the same costs as retailers. Again, sensitivity analysis has been used to account for the small sample size by increasing and decreasing the central estimate by 20%. It should be noted that the salary assumptions used to estimate the cash equivalent of this time have been adjusted to account for overhead costs

¹⁴¹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

Table 18 - Estimated cost of familiarisation with security labelling per organisation (A+B)

	Optimistic case	Central case	Worst case
Average cost per Manufacturer	£1,268	£1,585	£1,902
Number of Manufacturers	69	170	170
Total cost to Manufacturers (2019 prices)	£85,734	£264,037	£316,845
Average cost per Distributor	£1,341	£1,676	£2,011
Number of Distributors	9,085	14,685	14,875
Total cost to Distributors (2019 prices)	£11,936,470	£24,117,648	£29,315,630
Overall cost (2019 prices)	£12,022,205	£24,381,685	£29,632,474

Policy Option C - Mandatory security baseline

213. The same approach has been taken to estimate the familiarisation costs as with the labelling scheme options. However, the responses (in terms of estimated cost per organisation) differed for this policy option. Responses to this policy option suggest that costs per organisation will be higher:

- The RSM survey found that on average it would cost manufacturers £2,465, or 15.2 person days. The estimated retailer costs to read and understand proposed legislation are higher at £4,781.
- The cost to retailers includes four or five days for a director to familiarise themselves with the legislation as well as five to ten person-weeks for administrative, sales advisors and customer service staff.
- Similarly to the labelling scheme options, due to a relatively low response rate from both retailers and manufacturers, sensitivity analysis has been used to account for uncertainty in the estimates. To this end, the estimates have been increased and decreased by 20%. Similarly to previous estimates, it should be noted that the salary assumptions used to estimate these costs have been adjusted to account for overhead costs.

Table 19 - Estimated average cost of familiarisation with the initial three security requirements per organisation (C)

	Optimistic case	Central case	Worst case
Average cost per Manufacturer	£1,972	£2,465	£2,958
Number of Manufacturers	69	170	170
Total cost to Manufacturers (2019 prices)	£136,068	£410,632	£492,758
Average cost per Distributor	£3,825	£4,781	£5,737
Number of Distributors	9,085	14,685	14,875
Total cost to Distributors (2019 prices)	£34,050,277	£68,798,613	£83,626,507
Overall cost (2019 prices)	£34,183,612	£69,209,245	£84,119,265

7D(iii) - Estimating self-assessment costs

214. In addition to the one-off familiarisation costs outlined above, manufacturers of consumer connectable products will also have to undertake an assessment of their products (i.e to check which products are compliant and which are not) as part of their self-declaration to retailers. This declaration is mandatory under both Policy Option B - Mandatory security labelling scheme and Policy Option C - Mandatory security baseline.
215. Throughout the appraisal period all manufacturers will face a recurring self-assessment cost. For the purpose of this analysis, it has been assumed that this will occur on an annual basis. Similarly to the familiarisation-costs section, the RSM survey asked respondents to estimate the average number of person days per year that would be required to undertake self-assessment of compliance of their consumer IoT products, as well as the type of job roles that would be involved. This information was multiplied by the wages highlighted in [Table 17](#) in order to estimate the average cost per organisation and then scaled up by multiplying the cost per organisation by the estimated number of manufacturers in scope. It should be noted that all self-assessment costs have been adjusted to account for overhead costs.
216. On average, respondents said it would take around 30.1 person days per year and would mostly be the responsibility of IT or technical directors, managers and/or professionals. The cash equivalent of this time is estimated at £6,575. This represents the total overall cost per year for the organisation. This is the same across all policy options, which means the estimated costs under both mandatory policy options are the same. Again, as with the familiarisation costs methodology we have adopted, these costs have been inflated and deflated by 20% to account for the small sample size (£7,890 in the worst case scenario and £5,260 in the Optimistic scenario). As with the familiarisation costs, the salary assumptions used to estimate the cash equivalent of this time have been adjusted to employment costs to account for non-salary costs such as National insurance contributions.

Table 20 - Self-assessment costs for mandatory policy options (B+C)

	Optimistic case	Central case	Worst case
Average cost (2020 prices)	£5,260	£6,575	£7,890
Number of Manufacturers	69	170	170
Total cost (2019 prices, £m)	£5,154	£6,644	£7,732

217. In contrast to the mandatory options (Policy options B+C), self-assessment is not mandatory for **Policy Option A - voluntary security labelling scheme**. It has been assumed that only those manufacturers that will stand to gain from a security label (i.e those who already comply with the security requirements) will opt to undertake a self-assessment. The estimated number of manufacturers opting for a self-assessment in the central estimate is 1.8% (this is based on the number of manufacturers in the UK that are known to have adopted the voluntary code of practise. In the central scenario, it has therefore been estimated that 1.8% of manufacturers will take on the self-assessment costs. However, due to the uncertainty of this assumption sensitivity analysis has been used. It has been assumed that 1.8% of manufacturers adopt the label in the worst case and 0.27% in the optimistic case¹⁴².

Table 21 - Estimated annual self-assessment costs for manufacturers (A)

	Optimistic case	Central case	Worst case
Average annual cost per manufacturer (2020 prices)	£5,260	£6,575	£7,890
Number of manufacturers adopting voluntary label	0.27%	1.8%	1.8%
Total cost (2019 prices, £m)	£0.01m	£0.2m	£0.24m

7D(iv) - Estimating costs to retailers

Policy Option A and B - Labelling scheme options

218. It is possible that the introduction of a labelling scheme will also result in additional costs for retailers. The RSM survey identified two main costs for retailers that may result from the introduction of the mandatory labelling scheme:

- one-off familiarisation costs to retailers to read and understand the legislation (£1676)
- costs associated with the disposal of non-compliant goods (only relevant to the mandatory labelling option). Further information on the methodology used to estimate costs associated with the disposal of non-compliant goods is available in the subsequent section [7E\(iv\) - Estimating the costs associated with the disposal of non-compliant goods](#).

¹⁴² See footnote 107 for more detail on the rationale for this assumption.

Policy Option C - Mandatory security baseline

219. It is possible that the introduction of the mandatory security requirements, like the labelling scheme, will result in additional costs for retailers. As above, there will be a one-off familiarisation cost (£4,781) as well as costs associated with the 'disposal of non-compliant goods'. In addition to this, retailers will be required to verify a statement of compliance provided by the manufacturer (see the subsequent section [7E\(iii\) - Estimating the cost of publishing and verifying a statement of compliance](#)).

Table 22 - Direct cost to retailers under the preferred (C) and other shortlisted policy options (A+B)

	Optimistic case	Central Estimate	Worst case
Policy Option A - Voluntary Security Label	£12m	£24m	£29m
Policy Option B - Mandatory Security Label	£12m	£24m	£29m
Policy Option C - Mandatory Security Baseline ¹⁴³	£35m	£71m	£89m

7E - Cost methodology not of relevance to all options

7E(i) - Estimating the costs of labelling

220. Under the voluntary labelling scheme option (Option A) it has been assumed that the introduction of the scheme:
- will not place additional labelling costs onto manufacturers; or
 - increase costs for consumers.
221. These assumptions have been made for the following reasons:
- Firstly, it has been assumed that manufacturers will only adopt the label if the return on this investment exceeds the cost.
 - Secondly, due to the voluntary nature of this policy option, it has been assumed that adoption of the voluntary label will occur gradually, which will mean manufacturers incorporate the label into their business as usual updates to their packaging to minimise their costs. The average product development lifecycle is 1.5 years and packaging is redesigned on average every 30 months.¹⁴⁴ Therefore, in this scenario it has been assumed that costs will be incorporated as part of manufacturers regular update cycle and not passed onto consumers.

Policy Option B - Mandatory security labelling scheme

222. The cost of labelling will be incurred by all manufacturers of consumer connectable products selling their products on the UK market under Policy Option B. As the label is mandatory, some manufacturers may have to update their product packaging earlier than they otherwise would have as part of their usual packaging redesign cycle.¹⁴⁵ Therefore, it has been assumed that this will impose an additional cost on all manufacturers in scope.
223. There are different approaches manufacturers can take to implement the mandatory labelling scheme. For instance, manufacturers could opt for a stick on label or redesign their product packaging with the inclusion

¹⁴³ Note this does not include costs associated with the disposal of non-compliant stock (a potential indirect cost), which will impact both retailers and manufacturers. These costs have been presented as an overall cost to business. It has not been possible to separate the costs by manufacturer/retailer due to data limitations.

¹⁴⁴ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁴⁵ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

of the mandatory label. However, research on the cost of labelling changes for food manufacturers¹⁴⁶ states that it is unlikely that manufacturers would opt for a stick on label for the following reasons:

- 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.

224. In line with the evidence cited above, it has been assumed that manufacturers would incur a one-off cost of redesigning their packaging, rather than opting for a stick on label. In order to estimate the cost of redesigning packaging, DCMS has commissioned research into the cost of physical security labels and used research on the cost of food labelling and packaging changes as a guide. Previous research on the cost of food packaging changes can be found in [Table 23](#).

Table 23 - Evidence on the cost of product labelling

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

225. At the end of 2019, DCMS also commissioned research into the cost of implementing a physical security label on manufacturers of consumer IoT products. Six manufacturers responded to this question of the survey, reporting an estimated mean one-off cost of implementing a physical label of £100,630 (including one response of £500,000, representing 0.79% of the respondent's IoT turnover).¹⁴⁷

226. It should be noted that the information collected for this question included more responses from larger manufacturers than any other, with a wide range of responses from £3,000 - £500,000.¹⁴⁸ The mean one off cost is therefore likely not representative of the average manufacturer. Therefore, in an attempt to get a more accurate estimate, the cost of labelling was calculated by multiplying the average estimated number of product lines produced per manufacturer by the individual cost of updating packaging for a product line ([Table 23](#)). The total impact was estimated by multiplying the average cost per manufacturer by the estimated number of manufacturers in the UK. The optimistic estimate is based on information from the IoTUK Nation Database, which shows that in 2018 there were 69 manufacturers of computer, electronic and light electrical products in the UK.¹⁴⁹ Research conducted by RSM in 2020 found 170 manufacturers that sell their products to the UK market, which has been used as the central and worst case estimate for UK based consumer connectable product manufacturers.¹⁵⁰

227. For the purpose of this impact assessment, it has been assumed that the cost to manufacturers will be £3,517 on average per product line (2019 prices), where manufacturers redesign their external packaging. This estimate is based on the Campden BRI for DEFRA (2010) paper outlined in table 23, however, it is not clear from this paper that overhead costs had been accounted for and therefore, an overhead uplift of 22% has been added - bringing the total cost to £4,291 (see [Table 24](#)). The median and mean number of devices produced per manufacturer has been used for sensitivity analysis to estimate the total costs within the central and worst case scenarios. The cost to businesses will vary depending on the number of products that each firm manufactures.

¹⁴⁶ Developing a Framework for Assessing the Costs of Labelling Changes in the UK, Campden BRI for DEFRA, 2010 - <https://webarchive.nationalarchives.gov.uk/20130404011920/http://archive.defra.gov.uk/evidence/economics/foodfarm/reports/documents/labelling-changes.pdf>

¹⁴⁷ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁴⁸ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁴⁹ <https://datamillnorth.org/dataset/iotuk-nation-database>

¹⁵⁰ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

228. As the consumer connectable product sector is still relatively young, and new products are constantly coming onto the market, there is a lack of data on the number of different connectable products available. A survey of consumer connectable product manufacturers suggests that the median number of IoT product lines per manufacturer is 8, whilst the mean is 21 products.¹⁵¹
229. It should be noted that manufacturers will always have packaging and labelling costs that are not associated with regulation. The usual lifecycle of product packaging should be considered, as any changes implemented as part of this lifecycle can be incorporated into the business as usual redesign process, and can hence reduce any additional costs. This is likely to be the case for some businesses if there is an implementation period in which they have sufficient time to make changes to their packaging before the legislation comes into force. Many device manufacturers release upgraded versions of their products on an annual basis, leading to the design of new packaging, which could incorporate the mandatory security label. A survey of consumer IoT manufacturers found that the average product development lifecycle is 1.5 years and packaging is redesigned on average every 30 months.¹⁵²

Table 24 - Estimated labelling costs (Policy Option B)

	Optimistic case	Central Estimate	Worst case
Average labelling cost per product (2019 prices)	£4,291	£4,291	£4,291
Average number of products	8	8	21
Estimated cost per manufacturer (2019 prices)	£34,328	£34,328	£90,111
Estimated number of manufacturers	69	170	170
Total cost to UK consumer connectable product manufacturers (2019 prices)	£2.4m	£5.8m	£15.3m

7E(ii) - Estimating the cost of implementing security improvements

230. DCMS has engaged with industry to attempt to gather evidence on the cost impact of the three security requirements under Policy Option C - Mandatory Security Baseline through several channels, including the 2019 consultation, a manufacturer survey, and the 2020 call for views. The number of responses to the manufacturer survey, as well as the detail of information provided, varied for each of the three security requirements. For instance, little evidence was provided on the cost impact of removing default passwords but more detail was given on the cost impact associated implementing a vulnerability disclosure policy and security updates.
231. The approach to estimating these direct costs is the same as the approach outlined for the (i) familiarisation costs segment as well as the (ii) self-assessment segment. The average cost per manufacturer was first estimated and then this was scaled to the national level by multiplying the average cost per individual manufacturer by the estimated number of manufacturers in scope. Again, RSM survey data was used to estimate the average cost per manufacturer. The survey asked manufacturers to estimate the amount of staff time that would be required to implement changes associated with each security requirement and this was then multiplied by the wage rates highlighted in [Table 17](#), in order to estimate the financial cost of this time¹⁵³. It should be noted that the salary assumptions used to estimate the cost of staff time have been adjusted to account for non-salary costs (overhead costs).

¹⁵¹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁵² RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁵³ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

Vulnerability disclosure policies

232. The RSM survey revealed the difference in costs attached to the implementation of each security requirement but also the current level of compliance. Out of 16 respondents to the manufacturer survey, 12 (75%) stated that they already had a vulnerability disclosure policy¹⁵⁴. The results also show that the overall impact of mandating this Code guideline would be low or zero in many cases, however, even companies with a policy would bear some familiarisation costs to ensure that it was fully compliant with any legislation. On average, the estimated amount of staff time required to implement any changes as a result of legislation and provide a point of contact for reporting vulnerabilities for manufacturers where a change was required was 28.0 person days annually. The cash equivalent of this time (excluding the non-zero responses) is estimated to be £4,652 per manufacturer.

Security updates

233. According to the RSM survey, unlike the vulnerability disclosure policy, few manufacturers published a minimum length of time for which security updates will be provided. Out of 17 respondents only 4 provided this information to consumers for all their products. Mandating this (as in the preferred intervention - Policy Option C) will therefore potentially affect more of the market and be more time consuming to implement. According to data from Which? Investigations and the Which? Consumer test programme between October 2019 and January 2021, current compliance levels are just 2%. Therefore, across all scenarios it has been estimated that 98% of manufacturers will incur additional costs associated with implementing this security requirement.

- Findings from the RSM survey also indicated that the average amount of staff time required for compliance would be 91.4 person-days, mostly within IT professional/technical roles, and sales and marketing roles - amounting to an average annual cost of £17,631 per manufacturer, decreasing to an annual cost of £12,958 from year 2. Year one costs are higher because they account for additional costs associated with the implementation of this security requirement.

Default passwords

234. The market study and accompanying review of literature undertaken by RSM found very few products explicitly supplied with default passwords in the UK market, although in many cases the information on products did not confirm this either way. The manufacturer survey findings suggested that such products are now rare in the UK market: out of 17 respondents, only one (6%) indicated that any of their devices were produced with a default password. However, it is worth noting that due to the low response rate this survey is unlikely to be representative of all manufacturers of consumer connectable products. Therefore, data from Which? has been used to estimate the proportion of manufacturers that will be affected by this security requirement.
235. According to data from Which? Investigations and the Which? consumer test programme, around 10% of devices were found with 'default passwords', which has been used as a proxy for the proportion of manufacturers currently compliant with this security requirement. To this end, it has been estimated that this requirement will impose additional costs for 90% of manufacturers.
236. The RSM market survey did not return information on the cost impact associated with removing default passwords. DCMS attempted to gather further information on the costs that security requirements aligned to the top three Code of Practice guidelines would impose on organisations as part of the July 2020 call for views, but only two respondents provided information about the estimated annual cost to their organisations of implementing the requirement to ban universal default passwords, with varying degrees of context.
237. Without more robust data, the cost of implementing this security requirement has been estimated by taking the average reported cost of implementing a vulnerability disclosure policy and reporting minimum length of support for security updates. Hence, the estimated average annual cost used for this analysis is £10,918 and it has been assumed that this remains constant throughout the appraisal period. Sensitivity analysis has been applied to this estimate. The central estimate has been increased by 20% in the worst case scenario and decreased by 20% in the optimistic scenario.
238. [Table 25](#) summarises the methodology employed for estimating the cost to manufacturers of implementing the mandatory security baseline. The overall impact has been estimated by multiplying the estimated cost per manufacturer of each security requirement, by the estimated current level of compliance and then by the number of manufacturers in scope.

¹⁵⁴ This is likely an overestimate, the following IoTSF report "[Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report](#)" revealed that only 18.9% of companies have a vulnerability disclosure policy. This has been taken as the best estimate available. To this end, it has been estimated that around 81% of manufacturers will incur additional costs associated with implementing this security requirement.

Table 25 - Costs associated with Implementation of the Security Requirements (Policy Option C)

	Optimistic case	Central Estimate	Worst case
Security Requirement 1 - Ban universal default passwords			
% of Manufacturers that have to make changes	10%	10%	10%
Estimated number of manufacturers affected	7	17	17
Average annual cost per manufacturer (2019 prices)	£8,347	£10,918	£13,102
Total Cost:	£60,267	£185,606	£222,727
Security Requirement 2 - Implement a means to manage reports of vulnerabilities			
% of Manufacturers that have to make changes	81%	81%	81%
Estimated number of manufacturers affected	56	138	138
Average annual cost per manufacturer (2019 prices)	£4,559	£4,559	£4,559
Total Cost:	£254,803	£627,774	£627,774
Security Requirement 3 - Provide transparency on for how long, at a minimum, the product will receive security updates			
% of Manufacturers that have to make changes	98%	98%	98%
Estimated number of manufacturers affected	68	167	167
Average annual cost per manufacturer (2019 prices)	£17,277 in year 1 £12,958 from year 2	£17,277 in year 1 £12,958 from year 2	£17,277 in year 1 £12,958 from year 2
Total Cost:	£1.2m in year 1 and £0.88m thereafter	£2.9m in year 1 and 2.2m thereafter	£2.9m in year 1 and 2.2m thereafter
Overall Cost (all three security requirements, 2019 prices):	£12.2m	£30.4m	£30.8m

239. Overall, the estimated additional cost of implementing security improvements to meet the minimum security baseline in Policy Option C is £30.4m in the central estimate, £30.8m in the worst case and £12.2m in the optimistic scenario (2019 prices). The difference in cost is driven by the estimated number of manufacturers in scope and sensitivity analysis around the cost of implementing Security Requirement 1 ('ban universal default passwords'). The proportion of companies that incur additional costs as well as the cost per manufacturer of implementing the security requirements remain constant across the three scenarios.

7E(iii) - Estimating the costs of publishing and verifying a statement of compliance

Declaration of Conformity cost

240. Under the preferred option (policy option C), manufacturers are required to make a statement of compliance publicly available and provide retailers with this information. The estimated staff cost of providing security update information has been used as a proxy for the staff cost of providing a statement of compliance¹⁵⁵. As highlighted above, this accounts for overhead costs. The annual average cost, including detailed responses itemising the staff time, and direct estimates of total costs, is £12,958 per manufacturer. The overall cost of this scheme has been estimated by multiplying the average cost per manufacturer by the number of manufacturers within scope (170 is the best estimate and 69 in the high estimate), which brings the total cost (across all manufacturers) to £2.2m¹⁵⁶. The methodology for estimating this cost is summarised in [Table 26](#).

Table 26 - Declaration of Conformity costs (Policy Option C)

	Optimistic case	Central Estimate	Worst case
Estimated cost per manufacturer	£12,958	£12,958	£12,958
Estimated number of manufacturers	69	170	170
Total cost to UK consumer connectable product manufacturers	£0.9m	£2.2m	£2.2m

Verification of the Declaration of Conformity

241. Distributors of consumer connectable products, under policy option C, will be required to verify that manufacturers have published a statement of compliance. In order to estimate the cost of this obligation the following assumptions have been made:

- Firstly, it has been assumed that it will take a 'specialist manager' (or equivalent) within the organisation half an hour to verify that each product line has met the requirements.
- To estimate the cost of this time, data from the National careers average salary data has been used¹⁵⁷. The salary assumptions used account for non-salary costs such as national insurance costs.
- There is some uncertainty around the level of seniority of the employee required to check the statement of compliance. Therefore, the seniority of the employee has been varied across optimistic and worst case scenarios. In the optimistic scenario, it has been assumed that the verification only requires an 'Administrative' level role and in the worst case scenario it requires a 'Director' to verify the statement of compliance.

242. According to data from the RSM survey, retailers sell an average of 43 product lines which means it will take a Specialist Manager/Administrative role/ Director within the organisation approximately 21.5 hours to verify that all product lines meet the requirements. Using the above salary assumptions, the cost of this time to each retailer will be £585 and the overall cost (across all retailers) of this time amounts to £2m. These salary assumptions reflect employment costs (i.e account for overhead costs). The methodology for this estimate is summarised in [Table 27](#).

¹⁵⁵ This has been used as a proxy as the type of professionals involved in implementing the statement of compliance is expected to be similar to those required to provide security information along with the time required.

¹⁵⁶ manufacturers are expected to update the statement of compliance every 10 years and therefore this is expected to be a one off cost.

¹⁵⁷ See [Table 17](#) for salary assumptions.

Table 27 - Distributor Declaration of Conformity Verification Costs (Policy Option C)

	Optimistic case	Central Estimate	Worst case
Average staff level time per Distributor	21.5 hours	21.5 hours	21.5 hours
Hourly Wage Rate	£15	£27	£56
Average cost per Distributor (2020 prices)	£331	£585	£1,215
Number of Distributors	3,485	3,485	3,675
Total Cost (adjusted to 2019 prices)	£1.15m	£1.87m	£4.47m

7E(iv) - Estimating the Direct costs associated with the disposal of non-compliant goods**Policy Option B - Mandatory security labelling scheme**

243. Under this policy option, retailers in the UK would no longer be able to sell products without a security label which indicates whether the products meet the top three security requirements. Once legislation to this effect had been implemented, products that are non-compliant (don't have a security label) would not be able to be sold in the UK market.
244. Broadly, businesses (retailers and manufacturers) would face two significant costs that directly result from the disposal of non-compliant goods:
- a **loss of revenue** due to a higher proportion of consumer connectable products having to be disposed of; and
 - the **direct cost of disposal**.
245. In estimating the **potential loss of revenue** that might result from the disposal of non-compliant products, a number of assumptions have been made. In the central scenario it has been assumed that retailers will dispose of all current stock with a default password (of connected devices). As above, according to 253 Which? Investigations 10% of assessed consumer connectable products had a default password. This has been used to estimate the proportion of stock that will have to be disposed of in the central estimate. The banning of default passwords in consumer connectable products only accounts for one of the three security measures outlined, however, it serves as a good indicator for the proportion of stock that will likely have to be disposed of because, of the three security requirements in question, only the lack of default password is device-based and therefore runs the risk of a device needing to be disposed of. The remaining two security requirements are not device-based and can therefore be updated/changed even after devices have been sent to distributors. Consequently, it would be disproportionate to dispose of any product on the basis of compliance with Security Requirement 2 (Vulnerability Disclosure) or 3 (Transparency regarding security update support).
246. In reality, the central estimate of 10% is still likely an overestimate for several reasons:
- Firstly, rather than disposing of stock without a security label it is more likely that businesses will sell connectable products (without a security label) at a reduced price.
 - Secondly, the transitional period will give retailers (that do not hold large quantities of stock but rather receive new stock on an ongoing basis) time to sell stock. The estimated proportion of stock disposed of has been varied using sensitivity analysis, from 5% in the optimistic scenario to 45% in the worst case scenario.

247. In the absence of more recent information, data from Statista on Walmart inventory turnover from 2019 has been used as a proxy for average retail inventory turnover¹⁵⁸. This data underpins the estimated number of days it takes retailers to sell all inventory on hand.
- The estimated number of consumer connectable products sold per day by UK retailers was calculated by taking the number of 'new' products that would be purchased each year (see the preceding section [7Bi - Estimating the number of consumer connectable products](#)) and dividing it by the number of days in a year. For instance, in the central estimate it is estimated that 26m consumer connectable products will be sold in 2023.
 - Assuming that these sales are distributed equally among the 3,485 retailers, each retailer will sell an average of 7,338 products over the year or 20.1 products a day.
 - From this information, it is estimated that on average each retailer keeps 863 connectable products in stock. The estimate has been used for all three scenarios (worst case and optimistic).
 - The value of this stock has been estimated using RSM data on the price of consumer connectable products. Across the different product categories the average price per product has been estimated to be £295 (2019 prices) and from this the average value of each retailer's stock of connectable products totals £255,065.
248. [Table 28](#) summarises the methodology used to estimate the overall value of revenue lost. The overall loss of revenue amounts to £88m (2019 prices) in the central estimate (£421m in the worst case and £44m in the optimistic scenario). It should be noted that this is a one-off cost as with time it is expected that manufacturers/retailers will adjust to the new legislation.
249. Lastly, there is the direct cost associated with disposing of the non-compliant products. The RSM survey suggests the estimated cost of disposal reported by businesses ranges from £10-£50 per unit¹⁵⁹. The total cost of disposal has been estimated by multiplying the average unit cost of disposal (£30) by the estimated number of non-compliant units. Using this approach, it has been estimated that the cost to business, from the direct cost of disposal, amounts to £8.7m in the central estimate (£42m in the worst case and £4.4m in the optimistic scenario).

The environmental impact of disposing non-compliant goods

250. DCMS commissioned RSM International to estimate the environmental cost of disposal. However, while the direct cost to businesses from disposal has been estimated (see [section 7E\(iv\) - Estimating the Direct costs associated with the disposal of non-compliant goods](#)), the rapidly evolving nature of consumer connectable technologies makes it difficult to estimate its impact on carbon emissions and the wider environment. "Following a review of relevant literature, market research and the consumer, retailers and manufacturers survey, an adequate evidence base for costs could not be derived.¹⁶⁰" And although the Green Book provides guidance for calculating environmental costs, the proposed methodology for estimating changes in fuel usage and production of carbon requires baseline evidence on the level of energy required for the disposal of consumer connectable products "which is not present in the literature.¹⁶¹" That said, the literature does discuss the environmental impact of microelectronics, which includes a life-cycle assessment of consumer connectable products such as smartphones and tablets. According to this assessment, recycling accounts for just 1% of whole lifecycle greenhouse gas emissions, while production is the biggest contributor (around 80%).¹⁶²
251. In summary, under both policy option B and C the costs associated with the disposal are likely to include 1) the cost of disposing, recycling and reshipping non-compliant products; 2) loss of sales and therefore revenue from non-compliant products and 3) cost to the environment. However, for the reasons mentioned above it has at this stage not been possible to quantify the impact on the environment.

¹⁵⁸ <https://www.statista.com/statistics/1089067/walmart-inventory-turnover-rate-worldwide/#:~:text=Inventory%20turnover%20ratio%20of%20Walmart%20from%202018%20to%202019&text=In%20quarter%20four%20of%202019,billion%20U.S.%20dollars%20in%202020.>

¹⁵⁹ Note that as these are self reported costs it is reasonable to assume overhead costs have been accounted for. Therefore, to avoid double counting the costs estimated here, DCMS has not added an overhead uplift to this estimate.

¹⁶⁰ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁶¹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁶² Greenpeace. Guide to Greener Electronics, 2017.

Policy Option C - Mandatory security baseline

252. In estimating the potential loss of revenue that businesses may incur due to non-compliant devices having to be disposed of¹⁶³, the same approach has been taken as to the one described for the mandatory labelling scheme above.

Table 28 - Estimating the loss of revenue resulting from the disposal of non-compliant goods (Policy Options B + C)

	Optimistic case	Central Estimate	Worst case
Average Inventory Turnover	8.5	8.5	8.5
Estimated days it will take to sell Inventory on hand	43	43	43
Estimated number of products kept in stock	863	863	863
Average price of consumer connectable products¹⁶⁴	£296	£296	£296
Estimated value of retail stock	£255,066	£255,066	£255,066
Estimated number of retailers	3,485	3,485	3,675
Total value of stock	£889m	£889m	£937m
% of stock disposed of as a result of intervention	5%	10%	45%
Loss of Revenue:	£44m	£88m	£421m

7E(v) - Estimating the costs of enforcement

253. Under both policy option B and policy option C, an enforcement authority would be appointed. In estimating the enforcement costs, an assumption has been made that the enforcement costs will be identical across both policy options. This assumption has been made because we expect staff numbers and testing capacity to be identical across policy options. [Table 29](#) summarises the assumptions underpinning the estimation of enforcement authority staffing costs across all assessed options. The costs have been broken down into transitional costs and on-going annual costs across the following categories:

- **Staffing costs**
- **Overheads**
- **Testing costs**
- **Setup costs**

¹⁶³ Note that this cost also applies to manufacturers but due to data limitations it has not been possible to separate the cost out by manufacturers and retailers. Therefore, the overall market price has been used to capture the overall impact to businesses (manufacturer + retailer).

¹⁶⁴ Weighted to account for the varying level of popularity across the three product categories: Big ticket Items; Consumer lifestyle and connecting to the home.

Table 29 - Annual Staff Cost Assumptions

Grade	Annual Cost
EO	£36,177
HEO	£44,965
SEO	£54,270
G7	£68,918
G6	£89,073

254. As mentioned above, costs can be broken down into transitional costs and ongoing costs. Transitional costs include setup costs. Setup costs include staff costs as well as overhead costs. These costs are highlighted in [Table 30](#)¹⁶⁵.

Table 30 - Transitional costs

	EO	HEO	SEO	Grade 7	Grade 6	Total Costs
Core team	-	0.5	1	1.0	0.2	£81,743
Central	-	0.5	0.5	0.5	-	£42,038
Staffing total	-	1.0	1.5	1.5	0.2	£123,781
Overheads	-	-	-	-	-	£27,232
Testing Costs	-	-	-	-	-	£0
Overall Costs	-	-	-	-	-	£151,013

255. Ongoing costs can be broken down into (i) testing costs; (ii) staff costs and (iii) overheads costs. Testing costs will require the enforcement authority to purchase a range of consumer connectable products and then send them for external testing. The average value of a 'Big Ticket item' has been estimated at £736, while the average value of a 'consumer lifestyle' product has been estimated at £206. The average price of a 'connecting the home' product has been estimated at £114. External testing costs have been estimated at £100 per item. [Table 31](#) breaks down the number of products sent for external testing across product categories and across three scenarios:

Table 31 - Testing cost inputs

	Big Ticket	Consumer Lifestyle	Connecting the Home	Sent for External Testing	Total costs
Worst Case	50	50	50	54	£59,280
Central Estimate	35	35	35	36	£41,280
Optimistic Case	20	20	20	21	£23,640

¹⁶⁵ Overhead costs have been estimated in line with RPC guidance (i.e staff costs have been uplifted by 22%)

256. [Table 32](#) presents the ongoing costs across three different scenarios (worst case; central estimate; optimistic case). It should be noted that the different scenarios here are not based on the effectiveness of the enforcement approach but purley the costs. Therefore, the worst case scenario simply refers to the scenario with the highest expected costs and the optimistic scenario refers to a scenario in which the costs are lower.

Table 32 - Indicative ongoing enforcement costs

Worst Case						
	EO	HEO	SEO	G7	G6	Total Costs
Core Team	2.0	3.0	3.0	2.5	0.2	£560,169
Central	0.5	1.0	1.0	0.5	-	£151,782
Staffing cost	2.5	4.0	4.0	3.0	0.2	£711,951
Overheads	-	-	-	-	-	£156,629
Testing costs	-	-	-	-	-	£59,280
Overall costs	-	-	-	-	-	£927,860
Central Estimate						
	EO	HEO	SEO	G7	G6	Total Costs
Core Team	1.0	2.0	3.0	2.0	0.2	£444,568
Central	0.25	1.0	1.0	0.25	-	£125,509
Staffing cost	1.25	3.0	4.0	2.25	0.2	£570,077
Overheads	-	-	-	-	-	£125,417
Testing costs	-	-	-	-	-	£41,280
Overall costs	-	-	-	-	-	£736,774
Optimistic Case						
	EO	HEO	SEO	G7	G6	Total Costs
Core Team	1.0	1.0	2.0	1.0	0.2	£276,415
Central	0.25	0.5	0.5	0.25	-	£75,891
Staffing cost	1.25	1.5	2.5	1.25	0.2	£352,306
Overheads	-	-	-	-	-	£77,507
Testing costs	-	-	-	-	-	£23,640
Overall costs	-	-	-	-	-	£453,453

Section 8- Additional Analysis

8A - Analysis of the potential costs to consumers

8A(i) - Policy Option B - Mandatory security labelling scheme

257. A possible unintended consequence of mandating a physical label is the potential for additional costs to be passed onto consumers through higher prices. Three out of six respondents to a manufacturer survey said that they would pass on the cost of mandatory compliance labelling to the consumer, with two reporting that they would not pass on the cost and one expecting that they would pass on 1-10% of the cost.¹⁶⁶ However, it should be noted that the sample size for this question is low and therefore this is not representative of all manufacturers on the UK market.
258. The extent to which costs will be passed onto consumers will depend on competition as well as how significant the cost is relative to business turnover. To this end, the size of the business will likely affect the extent to which businesses pass on costs to consumers. Although the RSM research suggests that the cost of implementation as a share of consumer connectable product turnover will not be significant, this may not be the case for smaller firms¹⁶⁷. As a result, it has been assumed that all small manufacturers and small/micro retailers will pass direct costs onto consumers through higher prices. The IoTUK Nation Database has been used to determine the proportion of UK consumer connectable product manufacturers that are defined as 'small' and from this determine the extent to which costs will be passed onto consumers¹⁶⁸. It has been assumed, in the absence of more information, that 100% of the labelling cost will be passed onto consumers but that these costs will only be passed onto consumers in year 1 and thereafter be incorporated into business as usual costs. For instance, these changes may be incorporated into usual packaging updates.
259. It is estimated that 'small' manufacturers account for approximately 72% of IoT UK manufacturers (122) and 98% of retailers are small or micro sized businesses (3,405) (see [8B - Analysis of the impact on small and micro businesses](#)).
- Direct costs to manufacturers include (i) familiarisation costs; (ii) self-assessment costs; (iii) labelling costs and amount to £36,131 per manufacturer (£87,720 in the worst case scenario and £34,532 in the optimistic scenario).
 - Direct costs to retailers include (i) familiarisation costs and amount to £1,642 (£1,314 in the high scenario and £2,011 in the low scenario). The direct cost to manufacturers is expected to be higher in year 1, as manufacturers familiarise with the scheme but then drop off once manufacturers become familiar with the legislation.
 - In addition to the direct costs outlined above, direct costs resulting from the disposal of non-compliant goods will also impact both retailers and manufacturers. However, the exact distribution of this impact across manufacturers and retailers is unknown. To this end, table 32 presents the overall cost to consumers without and with the disposal of non-compliant goods included.
260. The overall cost to consumers has been calculated by multiplying the number of 'small' manufacturers and 'small/micro' retailers within scope by the average direct cost per manufacturer/retailer. Using this approach, the total cost to consumers (without the disposal of non-compliant goods) under this policy option is £10m in the best scenario (£6.2m in the optimistic scenario and £17.9m in the worst scenario). It is worth noting that this is a transfer from businesses to consumers rather than an extra cost.

¹⁶⁶ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁶⁷ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT](#).

¹⁶⁸ IoTUK National Database - <https://datamillnorth.org/dataset/iotuk-nation-database#:~:text=The%20IoTUK%20Nation%20Database%20brings,Things%20sector%20in%20the%20UK.&text=Organisations%20identified%20as%20part%20of,they%20used%20to%20describe%20themselves>.

Table 33 - Direct cost to consumers (Policy Option B - Mandatory security label)

Grade	Worst Case	Central Estimate	Optimistic Case
Total average direct cost to manufacturers	£34,532	£36,131	£87,720
Number of 'small' manufacturers	122	122	49
Aggregate direct cost to manufacturers	£10.7m	£4.4m	£1.7m
Total direct cost to retailers	£2,011	£1,642	£1,314
Estimated number of 'small' retailers	3,601	3,415	3,415
Aggregate direct cost to retailers	£7.2m	£5.6m	£4.5m
Overall cost to consumers (without the disposal of non-compliant goods)	£17.9m	£10.0m	£6.2m
Overall cost to consumers (including disposal of non compliant goods)	£480.8m	£106.6m	£55.0m

8A(ii) - Policy Option C - Mandatory security baseline

261. The same methodology and assumptions have been used to estimate the potential cost to consumers across both Policy Option B (Mandatory Security Label) and Policy Option C (Mandatory Security Baseline). The difference between the two estimates is in the direct costs to businesses. The direct costs to manufacturers for this policy option in year 1 amount to £52,201 (£55,505 in the worst case scenario and £48,598 in the optimistic scenario), and comprise:
- familiarisation costs;
 - self-assessment costs;
 - costs relating to the statement of compliance; and
 - costs associated with implementing changes related to the security improvements.
262. From year 2 direct costs to manufacturers comprise (i) self-assessment costs and (ii) costs associated with implementing changes related to the security improvements. In total these costs amount to £33,120 (£36,241 in the worst case scenario and £29,999 in the optimistic scenario) and remain constant throughout the appraisal period.
263. Direct costs to retailers are expected to be a one-off cost and comprise (i) familiarisation costs and (ii) costs associated with verifying the statement of compliance. These costs amount to £5,480 (£7,189 in the worst case scenario and £4,149 in the optimistic scenario).

264. Similarly to policy option B, costs associated with the disposal of non-compliant goods are also included. The overall cost to consumers with and without the costs associated with the disposal of non-compliant goods can be found within table 34.
265. Assuming that 72% of manufacturers are 'small' and 98% of retailers are 'small' the overall direct cost to consumers (excluding costs associated with the disposal of non-compliant goods) amounts to £65m in the central estimate over the appraisal period (£77m in the worst case scenario and £31m in the optimistic scenario). However, if the cost of disposal is included the overall cost rises to £162m in the central scenario (£540m in the worst case scenario and £80m in the optimistic scenario). As mentioned above, in estimating the costs to consumers, only the direct costs to manufacturers have been accounted for.

Table 34 - Direct cost to consumers (Policy Option C - Mandatory security baseline)

Grade	Worst Case	Central Estimate	Optimistic Case
Total average direct cost to manufacturers	£55,805 in year 1 falling to £36,241 from year 2	£52,201 in year 1 falling to £33,120 from year 2	£48,598 in year 1 falling to £29,999 from year 2
Number of 'small' manufacturers	122	122	49
Aggregate direct cost to manufacturers	£6.8m in year 1 falling to £4.4m from year 2	£6.4m in year 1 falling to £4.0m from year 2	£2.4m in year 1 falling to £1.5m from year 2
Total direct cost to retailers	£7,189	£5,480	£4,149
Estimated number of 'small' retailers	3,601	3,415	3,415
Aggregate direct cost to retailers	£25.9m	£18.7m	£14.2m
Overall cost to consumers	£76.9m	£65.4m	£31.4m

8B - Analysis of the impact on small and micro businesses

8B(i) - Proportionality of the small and micro business impact assessment

266. As detailed in [Section 6 - Proportionality approach](#), the department expects that key policy decisions to be taken as part of the secondary legislation development process will materially affect the impact this policy will have on businesses, consumers and the broader economy. The cost-benefit analysis detailed in this impact assessment is therefore indicative, and will be built upon in subsequent impact assessment publications, once details of remaining policy decisions are sufficiently mature to render it proportionate to expand our evidence base and analysis.
267. Specifically, it should be noted that secondary legislation policy decisions on scope could conceivably change the overall impact of this legislation on small and micro businesses relative to larger businesses. As noted in [Box 11](#), decisions on scope could conceivably change the indicative cost benefit analysis through altering:
- The number of small and micro businesses that will be impacted by this legislation; and
 - The overall impact of this legislation on small and micro businesses relative to larger businesses, as businesses that specialise in the manufacture or distribution of specific product classes may have different characteristics (e.g. average number of product lines, compliance rates)

268. DCMS will therefore build upon its analysis of the impact on small and micro businesses in future impact assessment publications when these policy decisions have been finalised. This publication would be submitted for RPC scrutiny before tabling the secondary legislation necessary to bring the product security measures in the PSTI Bill into force¹⁶⁹.

8B(ii) - Number and distribution of businesses in scope of the regulation

269. The department is unable to use the number of employees as a way to split businesses into different categories. This is because, despite attempts to gather this information (see [6A - Extent of analysis and further impact assessment publications](#)) the DCMS still does not have this data. Turnover is used to split businesses into different size categories because this information is available through the IoTUK database and is the best known available evidence. The challenge with breaking down consumer connectable product manufacturers by employee size is due to the fact that these businesses do not fall into one sector. However, the IoTUK brings together a snapshot of the current state of the businesses and organisations that make up the Internet of Things sector in the UK and uses turnover as a way to break businesses into different size categories.

270. According to data from the IOTUK database, there are 69 manufacturers within the UK Internet of Things sector that are manufacturers of computer, electronic and light electrical products, Of these, the turnover is reported for 53 manufacturers. Of these 53 manufacturers, 72% have an annual turnover of less than £10m.

271. The IOTUK database brings together a snapshot of the current state of the businesses and organisations that make up the Internet of Things sector in the UK. The database, however, does not contain information on the number of employees and splits business turnover into the following categories:

- **Less than £1 million**
- **£1m - £10m**
- **£10m - £25m**
- **£25m - £50m**
- **£50m - £100m**
- **£100m - £250m**
- **£250m - £500m**
- **£500m**
- **Not known**
- **Not relevant (for Universities)**

272. The IoTUK turnover categories do not perfectly align with the EU definition of an SME and therefore it has not been possible to distinguish between ‘Micro’ and ‘small businesses’. The IoTUK turnover also reports business turnover in sterling and not euros, however, for simplicity manufacturers with a turnover less than £10m have been defined as small (categories 1 or 2).

273. Using the above data, manufacturers have been split into three categories for the purpose of this impact assessment:

- **Small business** - Turnover less than £10m
- **Medium business** - Turnover between £10m and £50m
- **Large business** - Turnover over £50m

274. It should be noted that the sample size from the RSM research was considerably smaller than the information available in the IoTUK database and therefore the IoTUK distribution has been used as a best estimate. Assuming that the distribution of small; medium and large consumer connectable product companies is consistent across the entire population of 170 companies (as indicated in the RSM research), then approximately 122 companies would fall into the ‘small’ category defined above. [Table 35](#) details the methodology used for estimating the size distribution of UK consumer connectable product manufacturers.

Table 35 - UK consumer connectable product manufacturer size categories and distribution

Category	Definition	UK manufacturers for which turnover is reported in the IOTUK database	Estimated number of UK manufacturers
----------	------------	---	--------------------------------------

¹⁶⁹ This will be submitted to the RPC for scrutiny in the event that it passed the de minimis threshold.

Small business	Turnover less than £10m	38 (72% of total)	122
Medium business	Turnover between £10m and £50m	8 (15% of total)	26
Large business	Turnover over £50m	7 (13% of total)	22

275. It should be noted that the split between small, medium and large businesses derived using this methodology is consistent with the distribution identified by RSM which suggested that 65% of known UK consumer companies are small; 8% are medium sized and 27% are large.¹⁷⁰

8B(iii) - Do the impacts fall disproportionately on small and micro businesses?

276. It is possible that small manufacturers will be disproportionately affected by the introduction of policy option C as the majority of direct costs identified by DCMS are fixed costs and will therefore make up a higher proportion of turnover relative to larger manufacturers. To compare the impact of this policy on 'small' manufacturers relative to larger manufacturers the turnover of an archetypical / average manufacturer of consumer connectable products was estimated and compared to the expected turnover of a 'small' manufacturer.
277. An estimate for average turnover was calculated using the median turnover between the turnover categories outlined below, and multiplying the median turnover for each category by the proportion of manufacturers within each band to give a weighted average. Using this approach, the overall average turnover is £35.9m compared to £3.3m for 'small' manufacturers. The overall direct cost to manufacturers in year 1 amounts to £52,201 per manufacturer (not including costs associated with the disposal of non-compliant goods), but falls to £33,120 from year 2 of the appraisal period. In year 1, direct costs amount to 0.14% of average manufacturer turnover, but 1.59% of 'small' manufacturer turnover, and fall to 0.09% and 1% respectively from year 2 (assuming turnover remains constant throughout the appraisal period).
278. The aggregate impact on 'small' manufacturers is calculated by multiplying the number of 'small manufacturers' by the average direct cost (note this does not include costs associated with the disposal of non-compliant goods). In the best estimate this amounts to £6.4m in year 1 and £4.0m from year 2 of the appraisal period. In the high estimate (optimistic scenario), direct costs to manufacturers amount to £2.4m in year 1 and £1.5m from year 2. In the worst case scenario, year 1 costs amounts to £6.8m and £4.4m from year 2 (see [Table 37](#) for more details).

Table 36 - IoTUK Database Turnover Category Bands (central estimate)

Turnover Category	<£1m	£1-10m	£10-25m	£25-50m	£50-100m	£100-250m	£250-500m	£500m+
Median Turnover	£0.5m	£5.5m	£17.5m	£37.5m	£75m	£175m	£375m	£750m ¹⁷¹
Proportion of manufacturers in band	32%	40%	11%	4%	4%	8%	0%	2%

Table 37 - Direct cost as a percentage of manufacturer turnover

	Optimistic case	Central Estimate	Worst case
Direct cost as % of small manufacturer turnover	1.46% in year 1 falling to 0.9% from year 2	1.57% in year 1 falling to 1% from year 2	1.68% in year 1 falling to 1.1% from year 2

¹⁷⁰

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things_loT_products.pdf

¹⁷¹ Given there is no upper bound it has been assumed that the median turnover in this category is twice the £250-500m band.

Direct cost as % of average manufacturer turnover	0.13% in year 1 falling to 0.08% from year 2	0.14% in year 1 falling to 0.09% from year 2	0.15% in year 1 falling to 0.1% from year 2
--	--	--	---

279. Direct costs to retailers are expected to be lower and only occur in year 1 of the appraisal period. Direct costs to retailers include (i) familiarisation costs as well as (ii) costs associated with verifying a statement of compliance provided by the manufacturer.
280. In the best estimate, there are 3,485 retailers of consumer connectable products within the UK, and it is estimated that 98% are small or micro businesses (3415). Similarly to above, the total direct cost to retailers has been estimated by multiplying the average direct cost per retailer by the estimated number of retailers. The total direct cost to retailers amounts to £5,480 in year 1 with an estimated overall impact to small retailers of £18.7m (£14.2m in the optimistic scenario and £25.9m in the worst case scenario). The difference in the impact across scenarios is driven by differences in familiarisation costs.
281. Lastly, there are costs associated with the disposal of non-compliant goods which are expected to impact both manufacturers and retailers. In contrast to the fixed costs identified above, it is expected that costs associated with the disposal of non-compliant stock will vary by business size. For example, larger businesses will likely hold more stock and therefore risk more from a negative supply shock (larger quantity of stock disposed of). Despite the department's attempts to gather information on (i) the size of manufacturers and retailers of consumer connectable products, as well as (ii) data on their turnover¹⁷², due to a low response rate it is not possible to accurately predict the market share of consumer connectable products held by 'small/micro' businesses in the UK.
282. In the absence of this data, the market share held by businesses in the UK private sector with employees 0-49¹⁷³ (small/micro businesses) has been used as an indicator. To this end, it has been estimated that small/micro businesses account for (across retailers and manufacturers) 37% of the market share despite accounting for the vast majority of businesses. The market share held by small/micro businesses has been used to estimate the proportion of the impact resulting from the disposal of non-compliant stock that would fall onto small/micro businesses. In the best estimate, the total cost to 'small/Micro' businesses amounts to £36m (£18m is the optimistic estimate and £171m is the worst case estimate). It should be noted that this is expected to be a one off cost.

8B(iv) - Could Small and Micro Businesses be exempted while achieving the policy objectives?

283. The department does not consider that an exemption would be appropriate for Small and Micro businesses. This is because the effectiveness of the preferred policy option (policy option C) rests on a mandatory security baseline being embedded within every consumer connectable product in the UK. This is because a single insecure connectable product within a network undermines the security of all products connected to the network. An example of this is highlighted by news stories in 2017 regarding the exfiltration of 10GB of data from a casino, initially accessed through an insecure internet connected thermometer in a fish tank which subsequently provided access to other areas of the network¹⁷⁴. As outlined above, it is estimated that 'small' retailers account for a significant proportion of the consumer connectable product market (37%). With this in mind, exempting 'small' businesses from the proposed legislation (preferred option) will directly leave a significant proportion of the market vulnerable to cyber threats. Moreover, exempting 'small' businesses will indirectly leave devices that meet the baseline level of security vulnerable to cyber threats through the network effect described above. To this end, exempting 'small' businesses from this legislation will significantly reduce the effectiveness of the proposed policy and as a result leave consumers vulnerable. Ultimately customers of consumer connectable products should be able to expect baseline levels of cyber security irrespective of the size of the companies involved in the manufacture and distribution of the product that are made available to them.
284. The overall risk-profile of consumer connectable products made available to consumers by Small and Micro businesses does not differ materially from products made available by any other businesses. Irrespective of the size of the business, consumer IoT that fails to meet the baseline level of security being proposed leaves consumers vulnerable to cyber attacks. The potential for harm from cyber attacks and the types and severity of that harm to consumers is the same regardless of the size of manufacturer, retailer or retailer. Third party

¹⁷² RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁷³ <https://www.gov.uk/government/statistics/business-population-estimates-2019/business-population-estimates-for-the-uk-and-regions-2019-statistical-release-html>

¹⁷⁴ https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fnews%2finnovations%2fwfp%2f2017%2f07%2f21%2fhow-a-fish-tank-helped-hack-a-casino%2f

online marketplaces represent a significant aspect of the retail landscape. In a recent study, 64% of IoT devices were purchased from online marketplaces, which likely include platforms such as Amazon or eBay, and external research suggests that over half of products sold globally on the Amazon platform are from third-party sellers as of Q3 2020.¹⁷⁵ Small and Micro businesses' ability to use these platforms and distribution mechanisms means that the consumer demographics (including vulnerable consumers) to whom these products are made available, and so who are exposed to these risks, are wide and encompass the whole of the UK.

285. In the event that evidence emerged suggesting that the products made available to consumers by Small and Micro Businesses posed a lesser risk to consumers, it would be possible to adjust the scope of products covered by the proposed regulation. This would be done by Ministers, subject to agreement by Parliament. For more detail please see [Section 5B - Description of preferred option](#)

8B(v) - Could the impact on Small and Micro Businesses be mitigated while achieving the policy objectives?

286. We have committed to taking proportionate steps to mitigate any disproportionate impact this legislation and its enforcement would have on Small and Micro Businesses, without compromising the effectiveness of the legislation in meeting its objectives.
287. The department has considered the potential exemptions detailed in the RPC Small and Micro Business Assessment guidance¹⁷⁶. The mitigations we currently plan on incorporating within our approach are detailed below.

- **Transition period** - As noted in [Box 9 - Key details of policy positions underpinning the preferred intervention \(Option C\)](#), the Government will provide businesses with an appropriate grace period to adjust their business practices before the PSTI product security measures fully comes into force. Whilst specific timings are subject to change, active enforcement of this legislation is likely to commence no earlier than one year following royal assent. A response from a DCMS commissioned business survey suggest that a 12 month grace period would give businesses sufficient time to sell non-compliant stock¹⁷⁷. Additionally, there will be a period after introduction to parliament but before royal assent, commencement, and the transition period where industry will be able to view the legislation itself. In the early stages of the legislation being actively enforced, the department will ensure that the appointed enforcement authority takes into consideration the disproportionate impact of fixed costs on Small and Micro Businesses, when determining the most appropriate response to instances of non-compliance.
- **Information** - DCMS has produced multiple publications on its proposals as well as engaged and formally consulted with industry including Small and Micro Businesses across several years through the development of this legislation. The enforcing authority will provide support to relevant economic actors to enable them to comply with their duties under this legislation. Tailored information and guidance to assist Small and Micro Businesses in adjusting their business practice to comply with their duties will also be made available.
- **Assurance** - DCMS has also funded the development of an assurance scheme to provide an accessible means for start-ups and smaller businesses to show their commitment to protecting consumers from cyber threats¹⁷⁸. The enforcing authority will take into account the extent to which manufacturers have taken steps to improve the security of their products with available assurance offerings when investigating instances of non-compliance, and so the targeted action the department has already taken to catalyze the development of this scheme will enable smaller businesses to mitigate fixed costs such as those associated with familiarisation.

288. It should be noted that, as the analysis of the impact on Small and Micro Businesses included in this Impact Assessment is indicative and will be built upon in subsequent publications (see [6A - Extent of analysis and further impact assessment publications](#)), the list of mitigations detailed above is not final. The department will ensure that appropriate mitigations, commensurate to any disproportionate impact placed upon Small and Micro Businesses by this legislation are considered in subsequent impact assessment processes, and before any action is taken to bring this legislation into force.

¹⁷⁵ Sabanoglu, T, 2020, [Third-party seller share of Amazon platform 2007-2020](#)

¹⁷⁶ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827960/RPC_Small_and_Micro_Business_Assessment__SaMBA__August_2019.pdf

¹⁷⁷ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁷⁸ <https://www.gov.uk/government/publications/grant-programme-for-consumer-iot-assurance-schemes-202021>

8C - Break-Even Analysis

289. Break-even analysis has been undertaken to estimate the number of incidents that would have to be prevented under each of the policy options in order for the costs of implementing regulation to equal the benefits. The break-even point¹⁷⁹ is the point at which total cost and total benefits are equal. In our modelling the benefits arise from a reduction in the number of cyber attacks. Therefore, in this case, the break-even point highlights the number of cyber attacks/incidents that would need to be avoided / prevented for benefits to meet total direct costs.
290. Using this approach, the estimated number of avoided incidents needed for the preferred policy option to pay for itself amounts to 301,351 over the 10 year appraisal period, which translates to an average of 30,135 incidents annually. To put this into perspective, the Crime Survey for England and Wales recorded 2,993,880 incidents of cyber crime in 2019. This, as already mentioned, is likely a significant underestimate for the following reasons:
- Cyber attacks are often invisible
 - This data relies on respondents reporting incidents
 - This data only covers England and Wales. Assuming that the number of cyber crime incidents are in line with ONS population estimates (i.e only account for 88.9% of incidencies across the UK)¹⁸⁰ An estimate for the number of recorded incidents across the UK is 3,364,437.

Table 38: Break-Even analysis - Number of avoided cyber crime incidents needed over 10 year appraisal period

	Worst Case	Central Estimate	Optimistic Case
Voluntary Labelling Scheme	106,088	60,482	25,664
Mandatory Labelling Scheme	1,872,671	98,718	151,176
Mandatory Security Baseline	2,157,820	301,351	225,185

8D - Analysis of potential trade impacts

8D(i) - Policy Option B - Mandatory security labelling scheme

291. Under the scenario in which the mandating of the security label is the chosen policy option, UK production would not be significantly affected. The estimation of medium and long-term traded effects is based on a general equilibrium model simulation and conducted on the basis of the GTAP model by the Global Trade Analysis Project. The modelling suggests UK domestic industry output slightly increases across the board for the sectors affected by the policy measures. The highest relative increase is recorded for smart electrical equipment (+0.32%), followed by smart computer and electronic products (+0.3%)¹⁸¹.
292. UK production would be affected by higher regulatory costs, which in turn have an impact on UK suppliers' relative international competitiveness. The negative effects are only marginal though.
293. UK aggregate export volumes in the sectors affected by the policy measures would only marginally decrease. The highest decreases are estimated for the smart computer and electronic products sector and for smart electrical equipment (-0.21%)¹⁸².
294. UK aggregate import volumes in the sectors affected by the mandatory labelling scheme would also slightly decrease as importers would have to bear higher costs. The highest relative decrease is estimated for smart toys and video game consoles (-0.63%)¹⁸³. As the numbers reflect changes for a 5-year time horizon, the annualised numbers are negligible. This is also true for other sectors affected by the proposed regulations.

¹⁷⁹ The break-even point in economics, business—and specifically cost accounting—is the point at which total cost and total revenue are equal, i.e. "even". There is no net loss or gain, and one has "broken even"

¹⁸⁰ <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates>

¹⁸¹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁸² RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁸³ 132 European Commission (2019). Reflection on the Economic Modelling of free Trade Agreements. Chief Economist Note. Issue 2, 2019.

Bilateral imports from the UK's key trading partners are estimated to only slightly decrease in all sectors affected by the regulations.

8D(ii) - Policy Option C - Mandatory security baseline

295. Under the intended policy intervention, UK trade will be largely unaffected. This is because the highest relative impacts would likely result from costs relating to the disposal of non-compliant goods and these costs are expected to be only temporary. Beyond this, recurring costs are expected to be relatively small.¹⁸⁴ Furthermore, foreign suppliers are expected to amend their products to ensure they comply with UK regulations. The estimation of medium and long-term traded effects is based on a general equilibrium model simulation and conducted on the basis of the GTAP model by the Global Trade Analysis Project. The modelling suggests that UK industrial output would slightly increase the sectors affected by the policy measures with the highest relative increase for smart electrical equipment (+1.52%), followed by smart computer and electronic products (+1.42%)¹⁸⁵. It should be noted that these predicted changes would likely materialise within the first two years, however, the effects would likely phase out over the longer term as the recurrent compliance costs would be marginal. In terms of trade, UK aggregate export volumes are initially expected to decrease slightly for all product categories (from -0.56% for smart toys to -0.99% for smart electrical equipment)¹⁸⁶. In the short to medium term, the decrease in the UK's aggregate export volumes results from temporary lack of competitiveness of companies that import to the UK. However, as with the impacts on domestic output, after the first 2 years the effects are expected to phase out over the longer-term, leaving UK exports largely unaffected.
296. Bilateral imports from the UK's key trading partners are estimated to only slightly decrease in all product groups affected by the proposed regulations. The impacts are generally less pronounced than decreases in UK exports. Overall economic activity in the UK will remain largely unaffected by the proposed measures. UK trade volumes will only marginally decrease in response to the implementation of the policy measures. As mentioned above, the highest relative impacts would likely result from costs related to the disposal of non-compliant products, which are expected to be temporary.

8E - Equalities Impact Assessment

297. DCMS as a public authority has a legal obligation to consider the effects of policies on those with protected characteristics¹⁸⁷ under the Public Sector Equality Duty set out in section 149 of the Equality Act 2010. The Public Sector Equality Duty requires a public authority, in the exercise of its functions to:
- consider the need to eliminate unlawful (direct or indirect) discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010;
 - advance equality of opportunity between people who share a protected characteristic and those who do not share it; and
 - foster good relations between people with a protected characteristic and those who do not share it.
298. The Equality Duty is not an obligation to achieve a particular result, but rather a mechanism to eliminate unlawful discrimination, or to promote equality of opportunity and good relations between persons of different protected groups. It is a duty to have due regard to the need to achieve these goals.
299. There is reason to believe that regulation to require consumer connectable products to meet minimum security requirements will serve to promote equality. We expect the preferred option to raise the security standards embedded in devices, protecting consumers from the potential harms that may be caused by insecure products. The policy addresses current issues which users with protected characteristics may be particularly exposed due to variable awareness of the issues required to make informed decisions. Doing nothing may potentially expose vulnerable groups to a greater risk of experiencing a cyber attack. For example:
- Customers aged 75+ are the least likely to check whether a smart device has a default password (only 8% responded "Yes", compared to 20% across all consumers.)¹⁸⁸. When asked whether they have checked for a default password, those ages 75+ replied were the most likely to reply "Don't know" (14%), possibly reflecting their lack of knowledge of technology¹⁸⁹.

¹⁸⁴ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁸⁵ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁸⁶ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

¹⁸⁷ Age, disability, sex, gender reassignment, pregnancy and maternity, race, religion or belief and sexual orientation.

¹⁸⁸ Ipsos "Consumer attitudes towards IoT Security" report.

¹⁸⁹ Ipsos "Consumer attitudes towards IoT Security" report.

- Customers aged 75+ are the least likely to have checked for the minimum support period for devices (only 6% responded “Yes”) ¹⁹⁰.
 - Customers in the oldest age group are the most likely to spend less than one hour researching a product, with one in five saying they usually do no research before making a purchase ¹⁹¹.
 - Those earning £35,000+ usually spend more time researching a product than those earning less than £35,000 ¹⁹².
 - Around 8% of those earning less than £35,000 do not research before making a purchase, 5 percentage points lower than those earning £55,000+ ¹⁹³.
300. Furthermore, the policy, by providing a transparent route for external parties to report vulnerabilities, will help to protect consumers including vulnerable groups.
301. However, we expect that the higher production costs caused by the regulation will be transferred from small businesses to consumers through higher consumer prices. Therefore, young consumers (aged 25-34) are likely to be disproportionately affected by the regulation as they are the main consumers of consumer connectable products. For example:
- On average, young consumers tend to own more devices across more categories ¹⁹⁴.
 - Since the start of the COVID-19 pandemic, consumers aged 25-34 are the most likely to have increased their household’s use of smart devices (65%), followed by those aged 16-24 (61%) ¹⁹⁵.
302. Consequently, young individuals are likely to shoulder more of the cost burden, relative to the older generations. This may be particularly detrimental to them as young consumers also tend to earn less, relative to the older generations ¹⁹⁶. Thus, the aforementioned price increase may have a disproportionate impact on their spending money.
303. Although evidence suggests younger consumers are the main purchasers of consumer connectable products, research shows that individuals in the highest income bracket (£55,000+) are the most likely to have purchased a device since March 2020. ¹⁹⁷ Therefore, given that the top earners have been the main purchasers of these products, it should be easier for them to shoulder any potential future increase in the price of consumer connectable products. Although, as mentioned above - while small businesses may pass on some of the costs to consumers, we don’t expect medium/larger businesses to pass on any of this cost. ¹⁹⁸ Furthermore, while small businesses make up a significant portion of businesses they are unlikely to own the majority of the market share.

8F - Assessment of impact on innovation

304. Cyber security is at the heart of the government’s approach to digital technology, and plays a critical role in ensuring people and businesses can benefit from the huge opportunities of technology. However, in an age of digital transformation, security may be left behind. DCMS recognises the important role consumer connectable products play in many people’s lives as well as the opportunities they create for innovation. ¹⁹⁹ That said, as outlined throughout this impact assessment, the security built into many of these devices is often limited, which poses a significant risk. Therefore the Government’s intended approach is to ensure security is built into consumer connectable products while limiting disruption to relevant economic actors. It is possible that additional costs to industry resulting from the introduction of this regulation may reduce innovation in the short run. However, in the long run increased security and confidence in consumer connectable products will likely lead to an increase in demand for these products, which in return may encourage further research and investment into the sector. Furthermore, the proposed regulation should also incentivise businesses to find innovative and more efficient ways to improve the security of their products.

¹⁹⁰ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹¹ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹² Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹³ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹⁴ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹⁵ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹⁶ <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/agegroupshetable6>

¹⁹⁷ Ipsos “Consumer attitudes towards IoT Security” report.

¹⁹⁸ See section 8A for more details.

¹⁹⁹ <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf>

Section 9 - Monitoring and evaluation

9A - Evaluation of objectives

305. As noted in [Section 4 - Policy objective](#), the objective of this policy is to reduce the risk to consumers, networks, businesses and infrastructure of the range of possible harms that may arise from vulnerabilities and inadequate security measures in consumer connectable products (detailed in [Section 3 - Rationale for intervention](#)).
306. As expressed in [NCSC Statement 4](#) - the view of the UK's technical authority for cyber threats is that estimating the reduction in probability of a successful cyber attack that would result from implementing these measures is "*inherently challenging*" and that "*there is no quantifiable evidence to be able to gauge or analyse crime specific to consumer connectable products*". The fundamental challenges of directly measuring the variable that it is the objective of this policy intervention to alter necessitates that the success of the intervention be monitored indirectly using proxy variables.
307. It is the view of the NCSC (as expressed in [NCSC Statement 1](#)) that the implementation of the top three principles within the Code of Practice "*will make the most fundamental difference to the vulnerability of consumer connectable products in the UK*". This view was supported by the cyber security experts who contributed towards the development of the Code, and other key external stakeholders in feedback provided in the May 2019 consultation, and July 2020 call for views on regulatory proposals in this space.

9B - Proportionality of monitoring and evaluation considerations in this and future impact assessment publications

308. It should be noted that this primary legislation impact assessment principally relates to the product security measures in the PSTI Bill. As detailed in [5C - How the preferred option will be given effect](#), this measure will create a legislative framework that will enable Ministers to define key elements of the intended intervention using mechanisms including secondary legislation. These elements include the minimum security baseline that relevant economic actors will have to comply with, specific product classes in scope of the regulation, and the identity of the enforcing authority.
309. As detailed in [Section 6 - Proportionality approach](#), the department expects that key policy decisions to be taken as part of the secondary legislation development process will materially affect the impact this policy will have on businesses, consumers and the broader economy. The cost-benefit analysis detailed in this impact assessment is therefore indicative, and will be built upon in subsequent impact assessment publications, once details of remaining policy decisions are sufficiently mature to render it proportionate to expand our evidence base and analysis.
310. The minimum security baseline the legislative framework will seek to mandate will also be set out in secondary legislation. This initial baseline may also be updated in the future (see [5B - Description of preferred option](#)).
311. The most appropriate way to monitor the impact of a given version of the security baseline will be significantly impacted by the areas the requirements the baseline details relate to. For example, the existing monitoring provisions available to monitor compliance with the baseline, the technical feasibility of monitoring compliance with that baseline, and the external factors that will also impact on the success of the intervention will vary depending on the aspects of cyber security that the baseline principally concerns. For instance, the department expects that there are significant differences in the proportionality of pursuing efforts to monitor each of the three initial security requirements. The view of the NCSC on the proportionality of monitoring the initial security baseline is detailed in [NCSC Statement 7](#).
312. The department expects that secondary legislation defining the initial security baseline will be tabled alongside secondary legislation defining other outstanding elements, such as regulations detailing specific product classes excepted from scope. The Government will not commence elements of the product security measures in the PSTI Bill that would impose a material cost on relevant economic actors until secondary legislation setting out the initial security baseline comes into force.
313. Where appropriate, the Government will include review clauses in future secondary legislation that establishes or materially alters the minimum security baseline this intervention will mandate. Impact assessment publications accompanying the tabling of this secondary legislation will set out details of monitoring and

evaluation specifically relevant to the version of the security baseline being mandated, including the timings of subsequent post-implementation reviews.

NCSC Statement 7

Minimum security baseline monitoring challenges

“The overall objective of the proposed DCMS regulation is to improve the level of security embedded within consumer connectable products and through this protect UK citizens and businesses from cyber crime and cyber attacks. Evaluating compliance of the security requirements around vulnerability disclosure policies and transparency around how long products will be supported for will be realistically feasible, as this information will need to be made publicly available. It will be noticeably harder to evaluate compliance for the requirement on default passwords because it would be very difficult and disproportionate to assess every product entering the UK market. However, as noted in [NCSC statement 4](#), the NCSC acknowledges that there is no quantifiable evidence to be able to gauge or analyse crime specific to consumer connectable products. Therefore, without evidence on cyber crime specific to consumer connectable products, it is not possible to effectively evaluate the regulations impact in reducing cyber crime”.

314. Additionally, external factors that may affect the success of the intervention are likely to depend on the specific components of the security baseline being mandated. These may include factors such as the following:

- **Changes in the behaviour of malicious actors:** The top three principles within the Code of Practice, according to NCSC (see [NCSC Statement 1](#)), will make the most fundamental difference to the vulnerability of consumer connectable products in the UK. However, it is possible that these three requirements become less effective in protecting consumers if malicious actors develop new ways to exploit vulnerabilities embedded within consumer connectable products.
- **New threats:** It is possible that new threats emerge in the future which exploit vulnerabilities within consumer connectable products, which may potentially limit the security this intervention provides.
- **Technological Innovations:** The emergence of new classes of consumer connectable products as technological innovations enable an increasingly broad range of consumer products to connect to the internet could create additional risks from devices being compromised, or new incentives for malicious actors to target these products.
- **Changes to the domestic and regulatory landscape:** This policy initiative sits alongside a robust existing product safety framework, as well as a number of existing and planned regulatory initiatives affecting products in scope, both domestically and internationally. Whilst the Government will endeavour to ensure the legislative framework harmonises with these initiatives, changes to the broader regulatory landscape could impact the efficacy of the PSTI product security measures.
- **A short term increase in the number of insecure devices purchased.** There is a risk that leading up to the regulations coming into force, retailers may sell non-compliant products or products that would otherwise have a negative label at a reduced price, leading to an increase in the number of insecure products being purchased without customers being aware. This may also reduce the benefits in the short term.

9C - Indicative monitoring and evaluation considerations

315. The department expects that the monitoring approach outlined in future secondary legislation impact assessment publications will seek to establish proportionately robust systems for monitoring compliance with the security baseline being mandated in that secondary legislation. This could include (but may not be limited to) elements including:

- appropriate data from the appointed enforcement authority on variables related to compliance, such as volumes over time of reported and confirmation violations of obligations related to the implementation of the security baseline;
- the recurring assessment of existing external evidence regarding compliance (such as the publications and activity noted in [2H - Prevalence of baseline security measures](#)); and
- the commissioning of bespoke research and/or evidence gathering activity, (such as the collection of appropriate realised cost data) if proportionate for the version of the security baseline being mandated (as evidenced by the points in [NCSC statement 7](#), this is likely to vary depending on the security provisions mandated by the baseline).

Annex 1 - Top three consumer connectable product security guidelines

Annex 1A - Guideline 1 - No universal default passwords

316. Passwords are an easily-implemented, low-cost security measure. Most consumer connectable products will use a password, with the majority of these passwords being set to default during the manufacturing process. Possible permutations of default usernames and passwords could include “admin/admin”, “admin/0000”, “user/user”, “root/12345” and “support/support”²⁰⁰.
317. 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 connectable products because the default passwords can be found online and easily used to target and gain access to internet connectable products.
318. The implementation of default passwords that are present universally across multiple devices, or produced by an insufficiently sophisticated password generation mechanism that enables passwords to be easily derived or guessed, is a particularly concerning security vulnerability, as the compromise of one device can enable all devices using the same default password or password generation mechanism to be compromised.
319. This problem dates 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”²⁰¹.
320. A 2017 Keeper Security survey²⁰² 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 security²⁰³.

Annex 1B - Guideline 2 - Implement a vulnerability disclosure policy

321. Universal default passwords are one example of a broad suite of security vulnerabilities that can create opportunities for malicious attackers to commit cyber crime or disrupt user activity.
322. Although some vendors may seek to identify and remediate vulnerabilities before their devices and services are brought to market, testing for everything is impossible. As a result, once products come to market, vulnerabilities may still be found in physical devices and associated services, either through intentional investigation or accidental discovery.
323. 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.
324. 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.
325. 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.
326. 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 mature companies in the National

²⁰⁰ <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>

²⁰¹ https://www.theregister.com/2013/03/19/carna_botnet_ipv4_internet_map/

²⁰² <https://www.keepersecurity.com/blog/2017/11/22/survey-says-iot-toys-high-holiday-wish-lists-security-not-much/>

²⁰³ <https://www.keepersecurity.com/blog/2017/11/22/survey-says-iot-toys-high-holiday-wish-lists-security-not-much/>

Telecommunications and Information Administration survey²⁰⁴ 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.

327. In the absence of a vulnerability disclosure policy, security researchers may resort to disclosing security concerns publicly because they have no outlet to report vulnerabilities to the manufacturers of consumer connectable products. This is problematic because it may create reputational damage for the companies concerned, leave a window of vulnerability for consumers using those products, and impact confidence in the adoption of consumer connectable products overall.

Annex 1C - Guideline 3 - Security updates

328. Providing security updates in a timely manner is one of the most important mechanisms to protect consumers. Their purpose is to address security shortcomings that place consumer privacy, data and security at risk, specifically security shortcomings that are typically only identified, and able to be utilised by malicious actors, once the product is on the market.
329. When large numbers of devices share the same vulnerabilities, it becomes an effective strategy for attackers to include exploits for these vulnerabilities in self-propagating malware, such as Mirai, that are used to form large networks of compromised devices (botnets).
330. 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.²⁰⁵ 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 security updates also protect against future variants of attacks that exploit other vulnerabilities, neutralising their effect.
331. Security updates, and transparency from manufacturers on the length of time these updates will be provided for, can also enable consumers to make better informed purchasing decisions. If a consumer does not have transparency on how long a connectable product they purchase will be supported with security updates for, they are likely to continue using that product when it becomes unsupported.²⁰⁶ Even though this exposes them to higher risk of compromise from cyber criminals or other hostile actors.

²⁰⁴ https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

²⁰⁵ <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>

²⁰⁶ Ipsos Mori survey report

Annex 2 - Description of the policy development process, and other policy options considered

332. Following the publication of the Code of Practice for Consumer IoT Security (see the preceding section [2H - Previous UK Government Interventions](#)), the Government has been actively exploring a number of regulatory and non-regulatory options to address the challenges presented by insecure consumer connectable products.
333. In line with HMT Green Book guidance on options appraisal, a long-list of options for intervention in this area was initially considered. These are summarised in [Box 13](#) below.

Box 13 - Options considered for improving consumer connectable product cyber security

Options dropped after long-list appraisal process

- *Consumer awareness and behaviour change campaign*
- *Upstream interventions e.g. improving router and telecoms network security*
- *Standards & creating assurance schemes*
- *Legislating to ensure that consumer connectable products made available to UK customers comply with all 13 guidelines set out in Code of Practice for Consumer IoT Security*

Options dropped following consultation feedback

- *Mandatory consumer labelling scheme, with the label evidencing compliance with all 13 guidelines of the Code of Practice for Consumer IoT Security*

Options carried forward for shortlist appraisal, but not preferred

- *Option 0 - Do nothing*
- *Option A - Voluntary security labelling scheme (Do-minimum option)*
- *Option B - Mandatory security labelling scheme (Other viable option)*

Preferred option

- *Option C - Legislate to mandate a minimum security baseline for consumer connectable products, with this baseline initially aligning to the top three guidelines of the Code of Practice*

Annex 2A - Options dropped after long-list appraisal process

Annex 2A(i) - Consumer awareness campaign

334. It was concluded that a consumer awareness campaign would not be an appropriate method of achieving the policy objective. This is because although increased consumer awareness would help to reduce the problem of information asymmetry in the market, the burden would still be on consumers alone, who don't necessarily have the skills, technical knowledge, or ability to protect their connectable products against cyber criminals to the same extent as manufacturers. As mentioned in the preceding section - [2H\(i\) - Progress in eliminating Universal Default Passwords](#), a recent Ipsos MORI report commissioned by DCMS revealed that

only one in five consumers check their devices for default passwords or the minimum length of time a product will receive security updates.²⁰⁷ This implies that there may be more devices on the market with default passwords than the available evidence suggests.

335. NCSC currently provides resources on their website to help consumers and businesses to stay safe online. Additionally, NCSC leads the Government's Cyber Aware campaign which focuses on improving the basic cyber security behaviour of UK consumers. Both interventions rely on consumers seeking out this information, being willing to educate themselves, and ultimately acting on the guidance provided.
336. These interventions or similar interventions are not mechanisms for achieving this policy objective, because many products can't be made more secure after they have been sold due to the limited user interface, the lack of settings for changing passwords or administering security updates, and limited support provided by manufacturers. In their 2019 investigation into wireless security cameras²⁰⁸, Which? were unable to obtain a response from multiple manufacturers when security issues were found.
337. Without manufacturers providing clear information about device security features, that can be made available at the point of sale, consumers would still not be able to make informed decisions on the types of products that they should buy, despite a higher awareness rate of the problem²⁰⁹. This is because many security features cannot be identified just by looking at the product, for example the minimum length of time that security updates will be provided, so consumers would not be able to find the information themselves unless it is provided by the manufacturer. As manufacturers are under no obligation to provide this information to consumers, there is a limited extent to which increased consumer awareness can influence the provision of security updates, or indeed the prevalence of other security measures.

Box 14 - Information on consumer connectable product security features available to UK consumers

In 2019, researchers from the Dawes Centre for Future Crime at UCL analysed information available on security features in the product manuals and online web pages of 270 consumer connectable products being sold by one UK retailer. These 270 products were manufactured by 220 different manufacturers (UK and international). For 42 devices (16%), details were provided in product manuals and online webpages, For 62 devices (23%) these were only provided on online webpages, and for 66 devices in manuals only. However, for the remaining 100 devices, no materials were available online at all.²¹⁰

This research found that only 10% of product manuals and materials analysed included any cyber hygiene advice. For 30 of the 170 devices that had product manuals and materials, it was not possible to discern whether a default password was used or not. Consequently, of the total 270 products, there were 138 (51%) devices for which a consumer would not know if the device did or did not have a default password. This is concerning because it means in many cases, consumers would not know if they were buying a vulnerable product.

Software updates, on the other hand, were mentioned in the materials for 62% of the 170 products. However, security was only highlighted as a feature of software updates in 10% of these cases. Furthermore, none of these products provided details on the length of time for a minimum support period.

The lack of transparency in manufacturer security information highlighted in this research, with 100 of the 270 products (37% of the total sample size) not providing manuals or materials online, further demonstrates that it is difficult for consumers to determine the level of security features present in these products prior to purchasing them.

338. The lack of progress in improving the cyber security of consumer connectable products (see the preceding section - [21 - Prevalence of baseline security measures](#)) suggests that previous efforts to improve consumer awareness of connectable product security shortcomings have not had a significant impact in incentivising manufacturers to improve security through increased consumer demand for these features.
339. Even amidst further efforts to raise consumer awareness of inadequate security measures in consumer connectable products, because of the complex market failures in this space (detailed in the preceding section - [Section 3 - Rationale for intervention](#)), manufacturers may also still choose to manufacture products that

²⁰⁷ 'Attitudes Towards IoT security', Ipsos Mori, which is to be published in March 2021.

²⁰⁸ <https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/>

²⁰⁹ RSM, 2020. [Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.](#)

²¹⁰ Blythe, J.M., Sombatrung, N., Johnson, S., 2019. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? <https://osf.io/preprints/socarxiv/63zkt/>

do not have basic levels of security, leaving consumers no choice but to buy products that do not adhere to the security standards in the Code of Practice, despite their higher levels of awareness.

340. Research has shown that price is most often the main consideration in the purchasing decision-making process for consumer IoT devices.²¹¹ In the above scenario, price may, therefore, continue to drive consumer decision-making, despite consumers being more aware of the risks associated with insecure products, as it is the consumer's right to choose a lower level of security in order to maximise their utility. As a result of choosing cheaper products with lower levels of security built in, this could put others at risk of falling victim to cyber attack through connecting a vulnerable device to the network.
341. Therefore, DCMS and NCSC concluded that an awareness campaign would not significantly reduce the risk of consumers being impacted by the range of possible harms that may arise from insecure consumer connectable products in the long term.

Annex 2A(ii) - Upstream Interventions - Router and telecoms network security

342. It would not be feasible to mitigate all security risks presented by insecure consumer connectable products through upstream interventions such as improving the security of home routers or telecoms networks. Current technology does not allow for features to be built into routers so that they can address vulnerable features built into connectable products.
343. Whilst the Government is introducing a new telecoms security framework²¹² that will enable Ministers to regulate the security of telecoms network equipment, this intervention will not be sufficient to address the risks presented by vulnerabilities in connectable products. A device that had a default password or an unpatched vulnerability could still be accessed by a cyber criminal even if the security of the router or telecoms network was improved. For example, the WannaCry attack could only be partially mitigated through better network configuration, if devices could still communicate with each other directly they could be compromised.
344. Future plans will look at how to build upon the legislation by further improving the security benefits provided by home routers, but this will require development of new standards and protocols as well as implementations of novel technologies. The pace of standards development and the number of modifications to existing protocols that may be required will limit the impact of these interventions in the immediate future, and so interventions are required in the short and medium terms to address the harm to consumers as well as to mitigate against risks that a router wouldn't protect against.

Annex 2A(iii) - Assurance schemes

345. The Government recognises the importance of product assurance services in achieving good security outcomes for consumer connectable products. Product assurance schemes can provide consumers with a greater degree of confidence in the security of their product, and enable manufacturers to receive valuable feedback on the design and implementation of security measures in their products.
346. The UK Government has awarded grants to three companies to create assurance schemes for different consumer connectable product classes. These schemes will provide industry with the opportunity to certify products against security standards, particularly EN 303 645. Alongside this, the UK Government has worked with the British Standards Institute, UL, the IoT Security Foundation and other organisations to ensure that their certification products are based on the same standards.
347. Attempting to reduce the risks posed by consumer connectable products purely with further assurance interventions, such as providing further funding to incentivise the creation of more comprehensive assurance schemes, was not considered a viable option for shortlist appraisal. Further government action to stimulate the consumer connectable product assurance market alone, would not meaningfully address fundamental market failures, such as the misalignment of incentives or information asymmetries, that have precluded market forces from resolving the issue of insecure consumer connectable products to date. Although a greater availability of cyber security assurance schemes could enable conscientious manufacturers to provide higher quality product security information to consumers, it would do little to address the limited profit incentives for manufacturers to improve the security of their products in the first place.
348. It should be noted that whilst the Government does not consider action to stimulate the connectable product security assurance market sufficient alone to meet the policy objective for this intervention, assurance

²¹¹ Harris Interactive, 2019. [Consumer Internet of Things Security Labelling Survey Research Findings.](#)

²¹² <https://www.gov.uk/government/collections/telecommunications-security-bill>

schemes play an important role in the intended legislative framework (see the preceding section - [5B - Description of preferred option and plan for implementation](#), for further details).

Annex 2A(iv) - Legislating to ensure that consumer connectable products made available to UK customers comply with all 13 guidelines set out in the Code of Practice

349. In addition to the top three guidelines to which the initial security requirements in the PSTI product security framework will align, ten further security guidelines were detailed in the Code of Practice for Consumer IoT Security²¹³. The thirteen outcome-led guidelines published in the Code (summarised in [Box 8](#)) detailed practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services.
350. As detailed in the preceding section - [2H - Previous UK Government Interventions](#), these guidelines brought together what was widely considered to be good practice in IoT security, and were developed by DCMS and NCSC in collaboration with external cyber security experts, industry, academic institutions, and civil society organisations.
351. The option of legislating to immediately mandate a security baseline aligned to all thirteen Code of Practice guidelines was discounted during the longlist appraisal process. Consideration of the extent to which this option optimises social value in terms of the potential costs, benefits and risks (as per the Potential Value for Money Critical Success Factor in HMT Green Book Guidance) highlighted the following:
- The view of the NCSC, the UK's technical authority for cyber threats, is that the top three principles within the Code of Practice will “*make the most fundamental difference*” to the vulnerability of consumer connectable products in the UK (see [NCSC statement 1](#) for further details). This view is supported by the key industry stakeholders involved in the development of the Code of Practice. The appropriateness of the top three as a suitable cyber security baseline was also supported by respondents to the Government's 2019 consultation (See [Box 15](#) for further details) and 2020 call for views on regulatory proposals in this space.^{214 215}
 - Feedback received from industry and cyber security experts has highlighted the importance of legislation in this space being able to adapt in the face of the rapid technological innovation. The preferred intervention of legislating to mandate a security baseline that is initially less stringent than the thirteen Code of Practice guidelines is therefore intended to be adaptable, and does not preclude additional requirements from being added to the security baseline, if justified by the weight of available evidence, or changes to the broader landscape (see the preceding section - [5B - Description of preferred option](#), for further details). As the policy development process progressed, it therefore became clear that the preferred intervention, and a legislative approach which would eventually mandate a security baseline aligned to the thirteen Code of Practice guidelines, are not mutually exclusive policy options.
 - Forecasts of continuing rapid growth in the consumer connectable product installed base (see the preceding section [2A - Growth of consumer connectable products](#) for further details) strengthens the case for urgent government action, so that the cyber security of consumer connectable products being made available to UK customers can be improved as quickly as possible. The initial mandatory baseline should therefore comprise requirements that are readily implementable whilst being sufficiently effective in reducing the risks presented by these products. Whilst the other Code of Practice guidelines could reduce consumer connectable product vulnerabilities, they are not all universally applicable to products within scope, would be of limited effectiveness in the absence of a mandatory vulnerability disclosure policy, or effective software updates (see [NCSC Statement 1](#)), and would necessitate more time for relevant economic actors to familiarise themselves with the legislation and update their business practices to ensure compliance, as well as additional evidence gathering and analysis. It is therefore likely that an initial security baseline aligned to the thirteen Code of Practice principles would delay the earliest commencement of the intended legislative framework, delaying the earliest point at which the benefits of reduced cyber crime would materialise relative to the preferred intervention, as well as the earliest point at which the legislative framework could be used to build upon the minimum baseline, for example, with additional security requirements aligned to the Code of Practice guidelines.

²¹³ <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>

²¹⁴ DCMS, February 2020, [Government response to the Regulatory proposals for consumer Internet of Things \(IoT\) security consultation](#)

²¹⁵ DCMS, March 2021, [Government response to the call for views on proposals to regulate consumer connectable product cyber security](#)

Annex 2B - May 2019 consultation on consumer IoT security regulatory proposals

352. In May 2019, the Government launched a consultation²¹⁶ to gather feedback on policy options for improving the cyber security baseline for consumer Internet of Things (IoT) products.
353. This consultation ran from 1st May to 5th June 2019. A consultation stage impact assessment²¹⁷ was also published alongside the consultation. This detailed the Government's nascent rationale for intervention, summarised anticipated benefits and costs resulting from the regulatory options proposed in the consultation, and also requested further evidence to inform the ongoing policy development process.
354. A government response to the 2019 consultation was published on 27th January 2020, summarising the responses to the consultation questions and outlining the Government's approach to Consumer IoT cyber security going forward.²¹⁸ A summary of feedback received on the consultation proposals is available in [Box 15](#).

Box 15 - May 2019 IoT security regulatory proposal consultation

The 2019 Secure by Design Consultation ran from 1st May to 5th June 2019, and closed with 60 formal responses. It sought views from stakeholders on the following policy options:

	<i>Description</i>	<i>Consultation Outcome</i>
Consultation Option A	<i>Mandate retailers to only sell consumer IoT products that have an IoT security label (evidencing compliance with the top three Code of Practice guidelines)</i>	Carried forward for shortlist appraisal (Option A)
Consultation Option B	<i>Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines of the Code of Practice</i>	Carried forward for shortlist appraisal (Option C)
Consultation Option C	<i>Mandate retailers to only sell consumer IoT products that have an IoT security label (evidencing compliance with the thirteen Code of Practice guidelines)</i>	Dropped following consultation feedback

The consultation document set out questions around a number of aspects of the Government's proposed regulatory options. This included consulting on whether the Government should take powers to regulate the security of consumer IoT products. Other questions examined the Government's core proposals on how best to implement important security requirements within consumer IoT products, mindful of the risk of dampening innovation and avoiding placing a strong burden on manufacturers and retailers. All questions were open questions with participants having the opportunity to provide free text responses.

Consultation feedback summary

There were a variety of responses expressing their opinions on the options presented. Some respondents agreed with increasing transparency for consumers, while others highlighted that insecure products could still be purchased under the labelling options. For example, one respondent said that "there is a danger in pursuing Option A that the success of the labelling scheme outweighs the success of the core goal: to minimise the security risk of consumer IoT. Option B, which would mandate retailers

²¹⁶ DCMS, February 2020, [Government response to the Regulatory proposals for consumer Internet of Things \(IoT\) security consultation](#)

²¹⁷ DCMS, May 2019, [Secure by Design Consultation Stage Regulatory Impact Assessment](#)

²¹⁸ A full summary of the responses and the Government response can be found at: <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation>

to sell only products that meet the three security baseline, would go further in protecting customers from online threats.”²¹⁹

Key feedback themes summarised in the government response document are detailed below:

- **Regulation** - Many respondents were in favour of the government taking powers to regulate the security of consumer IoT products and the proposed legislative approach of mandating a minimum baseline.
- **Top 3 Security Requirements** - Many respondents agreed with the ‘top three’ security provisions (aligned with the top three guidelines from the Code of Practice) as an appropriate baseline for consumer connectable products, in particular there were a number of respondents who were supportive of the requirement to remove default passwords.
- **Security Label** - There were a wide range of responses to the proposed labelling option in the consultation, from those who agreed with a mandatory label to those who disagreed with its use to communicate requirements to consumers.
- **Effectiveness of Physical Product Labels** - Concerns were raised in responses to the consultation around the effectiveness of a physical product label. One respondent said that “A static one-size-fits-all label added as a tag to the product or a system cannot realistically cover the array of current and future IoT technologies and provide details on the potential risks attributable to them. Security cannot be simply and accurately gauged using conventional means, unlike an energy-efficiency label on a washing machine, for example.” Meanwhile, others suggested using an ‘online or ‘live’ label to account for the dynamic nature of cyber security.”²²⁰

Annex 2B(i) - Consultation stage impact assessment and further evidence gathering

355. The consultation also asked for additional details of estimated costs for the proposed options in the consultation impact assessment, to help improve the evidence and assumptions used in the analysis. Key evidence gaps identified in the consultation impact assessment included evidence on the cost to businesses and the reduction in the harm to consumers from improved product security as a result of the proposed regulatory options.
356. Unfortunately, there were not enough responses to these questions to provide the level of evidence required for the final stage impact assessment. Consequently, DCMS commissioned two research projects to fill these gaps: ‘Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape’²²¹ and ‘Evidencing the cost of the UK Government’s proposed regulatory interventions for consumer IoT’.²²²
357. The findings from these research projects have been used to inform the cost-benefit analysis within this impact assessment. It should be noted that the response rate for the business surveys as part of these projects was low (only 22 consumer IoT manufacturers and 12 retailers responded) even though the external supplier approached over 2,000 companies. The findings are therefore not representative of the broader UK business population, and therefore caution should be used in interpreting these results.

Annex 2C - Options dropped following consultation feedback

Annex 2C(i) - Mandatory consumer labelling scheme, with the label evidencing compliance with all 13 guidelines of the Code of Practice for Consumer IoT Security.

358. The option of a mandatory labelling scheme that would expect manufacturers to evidence the extent to which their products complied with all thirteen Code of Practice guidelines was presented to external stakeholders in the 2019 consultation and consultation stage impact assessment (Consultation Option C).
359. Consultation feedback highlighted that many of the same challenges that had informed the decision to limit the initial security baseline to the top three guidelines of the Code of Practice for mandatory implementation options, also applied to the selection of a security baseline for the labelling options the Government was considering (see the preceding section - [Annex 2A\(iv\) - Legislating to ensure that consumer connectable](#)

²¹⁹ DCMS, 2020. [Government responses to the Regulatory proposals for consumer Internet of Things \(IoT\) security consultation.](#)

²²⁰ DCMS, 2020. [Government responses to the Regulatory proposals for consumer Internet of Things \(IoT\) security consultation.](#)

²²¹ CSES, 2020. [Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things \(IoT\) Landscape.](#)

²²² RSM, 2020. [Evidencing the cost of the UK Government’s proposed regulatory interventions for consumer IoT.](#)

[products made available to UK consumers comply with all 13 guidelines set out in the Code of Practice](#) for further details). Many respondents to the consultation agreed that the top three security provisions set out in the consultation stage impact assessment (aligned with the top three guidelines of the Code of Practice) constituted an appropriate baseline for consumer IoT products. Respondents also highlighted the importance of adopting a staged approach to regulation.

360. Feedback from the consultation, as well as from technical experts, concerning the complexities of implementing some Code of Practice guidelines (as well as the additional complexities of mandating a labelling scheme evidencing compliance with requirements that do not universally apply to all products in scope) made it clear that a labelling scheme featuring a minimum security baseline broader than the top three guidelines would likely delay the earliest possible commencement of any labelling option. Additionally, limited evidence was submitted as part of the consultation to suggest that a baseline aligned to thirteen Code of Practice guidelines would improve security enough to offset the impact of this delay. Considering the above, the criticality of urgent action to reduce the risks associated with these products, and the Government's intent to adopt a staged approach to regulation (which wouldn't have precluded bringing additional requirements into the scope of the labelling scheme), this option was not carried forward for shortlist appraisal.

Annex 2D - July 2020 call for views on proposals for regulating consumer connectable product cyber security

361. To further augment the Government's policy development approach, and to gather additional external feedback on the option of mandating a security baseline, in July 2020 DCMS launched a call for views²²³. This sought feedback on proposals to regulate the cyber security of consumer connectable products by mandating a baseline aligned to the top three guidelines of the Code of Practice.
362. In March 2021, the Government published a response to the call for views²²⁴, summarising the feedback provided, and outlining details of the Government's intended regulatory intervention (Option C). Further details of the Government's intended policy intervention are available in the preceding section - [5B - Description of preferred option](#). A summary of feedback received on the call for views proposals is available in [Box 16](#).

Box 16 - July 2020 call for views on proposals for regulating consumer smart product cyber security

A call for views on regulatory proposals for mandating a minimum cyber security baseline for consumer smart products (**consumer connectable products**) made available to UK customers ran from 16th July to 6th September 2020.

Overall, the call for views received 110 responses. 74 responses came from organisations, and 36 from individuals. Of the organisational responses, the majority came from respondents who identified as "Producers" of consumer smart products (24%), cyber security providers (24%) and "Distributors"/sellers of consumer smart products (17%). Of the individual responses, the majority came from cyber security professionals (33%), followed by academics (22%) and professionals in other sectors (14%).

In addition to demographic information to aid in the analysis of feedback, the Government requested that respondents consider thirteen questions related to different aspects of its regulatory proposals, including the following key elements:

- **Scope of the proposed regulation** - including the approach to defining and maintaining product in scope, and whether conventional IT products (Laptops, desktop computers and Smartphones) should be included
- **Security Requirements** - including feedback on a mandatory baseline aligned to the top three guidelines of the Code of Practice
- **Obligations on economic actors** - including feedback on proposals to obligate distributors to play a role in ensuring that insecure products are not made available to UK customers, in addition to manufacturers
- **Enforcement approach** - including feedback on the appropriateness of various corrective measures, sanctions and powers that could be made available to the enforcement authority, as well as criteria for selecting an enforcement authority

²²³ DCMS, July 2020, [Proposals for regulating consumer smart product cyber security - call for views](#)

²²⁴ DCMS, March 2021, [Government response: Call for views on proposals to regulate consumer connectable product cyber security](#)

The Government also requested that organisations affected by the proposed legislation provide information regarding the likely impact of the proposals on their operations, to supplement the data gathered following the 2019 consultation (see [Annex 2B\(i\) - Consultation stage impact assessment and further evidence gathering](#)).

Call for views feedback summary

The table below summarises feedback to call for views questions related to key elements of the Government's proposed regulatory approach. Further details can be found in the Government Response document published in March 2021²²⁵.

Key feedback received	Key outcomes
<p>Scope - inclusion of conventional IT products <i>Strong overall support for the inclusion of conventional IT products, but qualitative feedback highlighted unique challenges that legislation would impose on the manufacturers of laptops and desktop computers (e.g. supply chain complexity)</i></p>	<p><i>Exclusion of laptops and desktop PCs from scope at commencement, with further industry engagement to be conducted before any action would be taken to add these devices to scope. Smartphones however, will be included from the commencement of the legislation</i></p>
<p>Scope - overall scope approach <i>Overall support for the proposed scope approach of using a broad definition of network-connectable product classes, specifying categories of products out of scope as necessary.</i></p>	<p><i>Adoption of the policy approach proposed in the call for views</i></p>
<p>Security Requirements <i>Broad support for the proposed security requirements (aligned to the top three Code of Practice guidelines), with additional feedback themes including an emphasis on the importance of any legislation aligning with internationally agreed standards.</i></p>	<p><i>Adoption of the security requirements approach proposed in the call for views, with the creation of an additional route to legal compliance where manufacturers have the option of complying with external standards specified by Ministers as a means of demonstrating compliance with the security requirements specified in the intended legislative framework.</i></p>
<p>Obligations - placing obligations on distributors <i>Majority support for the distributors of consumer connectable products being obligated to play a role in ensuring that non-compliant products are not made available. Some respondents highlighted the challenges that may arise from allowing manufacturers to decide how best to provide compliance information to distributors.</i></p>	<p><i>Adoption of the policy approach proposed in the call for views. In response to the feedback around the challenges that may arise from a lack of compliance information standardisation, the Government will mandate that manufacturers ensure a statement of compliance accompanies in-scope products.</i></p>
<p>Enforcement <i>Broad support for the example corrective measures, sanctions, and powers included in the call for views proposals, as well as the selection criteria for appointing an appropriate enforcement authority</i></p>	<p><i>Continued policy development aligned to the high-level approach included in the call for views</i></p>

Annex 2E - Development of labelling scheme options

363. To assist in the analysis of 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

²²⁵ DCMS, March 2021, [Government response: Call for views on proposals to regulate consumer connectable product cyber security](#)

assess the influence of different (security-related) labelling schemes on consumer choice for consumer IoT products.²²⁶ Further details of this study and its findings are presented in [Box 17](#).

Box 17 - Key findings from “The impact of IoT security labelling on consumer product choice and willingness to pay” (UCL Dawes Centre for Future Crime consumer survey study)

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 were tested. The survey results indicated that:

- 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 smartwatch or fitness tracker), 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.

364. The findings of the Dawes Centre for Future Crime study ([Box 17](#)) suggest that security labels can have a positive effect on consumer choice regarding the selection of products with additional security features. However, despite participants' willingness to pay more for security labels on average across the four products tested, functionality generally had a larger influence on choice. Moreover, the effectiveness of the label depends on the type of label used.²²⁷
365. Similarly, a 2005 study on eco-labelling of electrical products identified that consumers were willing to pay 30% more for an A rated washing machine, compared to a C rated washing machine and 60% more for an eco-friendly light bulb. However, participants also stated a preference for premium brands over non-branded products, and were willing to pay an additional 50% for a premium washing machine, exceeding the influence of the eco-label.²²⁸
366. Research conducted for Defra on the effectiveness of environmental labels suggests that the success of food eco-labelling schemes depend to a large extent on consumer awareness of the issue, in order for the label to result in consumer behaviour change.²²⁹
367. 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.²³⁰ A link has also been identified between nutrition knowledge and label use.²³¹ Research on the proportion of consumers who use labelling information to make healthier food choices is summarised in [Table 38](#).

Table 38 - Evidence on the effectiveness of food labelling on consumer choice

Title	Author	Findings
Impact of food labelling systems on food choices and eating behaviours: a systematic review and meta-	Cecchini, M., and Warin, L. (2016)	Food labelling would increase the amount of people selecting a healthier food product by about 17.95% (confidence interval: +11.24% to +24.66%).

²²⁶ 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/>

²²⁷ 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/>

²²⁸ Sammer, K., and Wüstenhagen, R. (2005). The Influence of Eco-Labelling on Consumer Behaviour – Results of a Discrete Choice Analysis https://www.alexandria.unisg.ch/4941/1/A07_Sammer_Wuestenhagen_BSE_2006.pdf

²²⁹ [Effective approaches to environmental labelling of food products](#), University of Hertfordshire, 2010.

²³⁰ Study on the Impact of Food Information on Consumers' Decision Making, TNS European Behaviour Studies Consortium, 2014.

²³¹ The effects of nutrition knowledge on food label use. A review of the literature, Miller, L., Cassidy, D., University of California, 2015.

analysis of randomized studies. <i>Obesity Reviews</i> , 17: 201–210.		
Study on the Impact of Food Information on Consumers' Decision Making	TNS European Behaviour Studies Consortium (2014)	Trans fat labels didn't consistently lead to healthier choices. Calorie labels led to 16% of people 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 in alcohol consumption on specific occasions. 17% stated a long term willingness to reduce alcohol consumption, however, other factors had greater influence on this decision than information labels.
Identifying Food Labeling Effects on Consumer Behavior	Araya, Sebastián & Elberg, Andres & Noton, Carlos & Schwartz, Daniel. (2018).	A study of the impact of the introduction of mandatory food labelling in Chile. Tested choice in cereals, chocolate and cookies. Found 12.5% less likely to buy cereals with warning labels but no effect on other categories, as expecting to find warning labels on unhealthy foods and less likely to be able to substitute away from negatively labelled products in these categories.

368. The available evidence suggests that food labels generally have a positive effect on consumers' food choices. However, the research detailed in [Table 38](#) suggests that other factors may also influence the effectiveness of labels in encouraging positive consumer behaviour, for example previous knowledge, interest in improving health and availability of healthy substitutes. Socio-demographic characteristics could also affect an individual's ability to understand some types of front of packaging labels, although not in all cases.²³²
369. It has also been found that the type of label used on the front of packaging affects the outcome of consumer food choices. The traffic light system has been found to be slightly more effective in enabling healthier food choices than other types of label,²³³ by helping to guide consumers towards important information.²³⁴ However, other research has shown that consumers can find labels confusing due to 'information overload', with 40% of consumers in one study unable to identify the healthier product when comparing two products using the traffic light system.²³⁵
370. A Better Regulation Executive and National Consumer Council report on the impact of regulated information on consumer behaviour and markets suggests that consumers can become overwhelmed by information, which reduces the effectiveness of the intervention in achieving the government's objectives. It also highlighted that understanding complex information was a challenge faced by vulnerable groups.²³⁶
371. Processing information provided by manufacturers is not costless for consumers, who must make a decision of when it is optimal to stop searching for a product and decide whether or not to make a purchase. Manufacturers must also take this into account, and hence there is an optimal level of information that suppliers would want to provide their customers in order to maximise their sales. Research has found that it is never optimal to provide the maximum amount of information to consumers, but rather the optimal amount of information depends on the value consumers place on the product before they initiate their search.²³⁷

²³² Malam, Sally & Clegg, Sue & Kirwan, Sarah & McGinjal, Stephen. (2009). Comprehension and Use of UK Nutrition Signpost Labelling Schemes.

²³³ Cecchini M, Warin L. Impact of food labelling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies.

²³⁴ Jones G, Richardson M. An objective examination of consumer perception of nutrition information based on healthiness ratings and eye movements. *Public Health Nutr.* 2007;10:238–44.

²³⁵ Leek S, Szmigin I, Baker E. Consumer confusion and front of pack (FoP) nutritional labels. *J Cust Behav.* 2015;14:49–61.

²³⁶ Better Regulation Executive and National Consumer Council, (2007). Warning : too much information can harm: an interim report on maximising the positive impact of regulated information for consumers and markets.

²³⁷ Fernando Branco, Monic Sun, J. Miguel Villas-Boas (2016) Too Much Information? Information Provision and Search Costs. *Marketing Science* 35(4):605-618. <http://dx.doi.org/10.1287/mksc.2015.0959>

Annex 2E(i) - Considerations for applying a labelling scheme to consumer connectable product security

372. Consumer connectable products are already subject to product safety regulations, requiring manufacturers to provide safety information to consumers either on the product itself or on the packaging. Examples under current EU regulations include the CE mark, Energy labels (appliances), Waste Electrical and Electronic Equipment Directive, Toy Safety Directive and the e-mark.²³⁸
373. As previously discussed, the efficacy of a label also depends on consumer awareness and the prioritisation of security when purchasing a consumer connectable product. DCMS commissioned a labelling survey of 6,482 consumers in January 2019 which included a question on the top four most important types of information for participants when buying smart devices.
- Three quarters (76%) of respondents noted cost, 72% reported functionality, whilst nearly half (49%) of participants consider security features to be important in their decision-making process, above other factors such as brand reputation, customer reviews, privacy features and design.²³⁹
 - This 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.²⁴⁰
 - It should be noted that, on first sight of the labels used in this study, only 23% of respondents identified that the presence of a label indicated that the product had some level of security.
374. Evidence suggests that labels can be effective in nudging consumers to change their behaviour, in this case to choose more secure consumer connectable products. However, although many consumers report security being a top priority, the effectiveness of a labelling scheme would be reliant on parallel efforts to equip consumers with the knowledge or information needed to be able to make informed purchasing decisions.
375. Research has found that many consumers purchase their smart devices online, where they wouldn't have access to the physical box. A Harris Interactive survey found that 37% of people mainly purchase their consumer IoT devices online and 33% mainly from retailer stores.²⁴¹ Another consumer survey found that on average 74% of consumers purchase online, and 18% purchase in store (60% buy big ticket items online, 77% connecting the home devices).²⁴² One large organisation in response to a manufacturer survey also highlighted that on-product packaging "*was of decreasing relevance*" as consumers often do not see this online or in a showroom, and that "*online information was much easier to deploy as it could be updated remotely*".²⁴³
376. As awareness of cyber security is thought to be currently lower than that of nutrition or the environment, it is expected that a security label will not have as great an impact on consumer decision making as food or eco-labels without parallel efforts to increase consumer awareness. As a result, it may take longer for security labels to become effective at incentivising behaviour change, as awareness of cyber security of connectable products increases.
377. Without a substantial awareness campaign, consumers may not understand what the label is telling them, and therefore ignore the information. Without an increase in consumer awareness, this would not lead to the benefits resulting from consumer pressure to improve security standards, and therefore there will be a lack of incentives for manufacturers to improve the security of their products.
378. As consumers are already provided with a lot of information when purchasing products, any additional security information would be competing with information on product features and safety. Consumers may be discouraged from taking into account this information due to the amount of information that they have to process in making a purchasing decision. Functionality and price are also important to consumers²⁴⁴, so an additional label may only be effective for consumers where security is already a priority or where they have prior cyber security knowledge.
379. A possible unintended consequence of a labelling scheme is that it could lead to consumers assuming a false sense of security of their products with a positive label, known as the 'halo effect'. This was a concern which was expressed in responses to the 2019 consultation, which suggested labelling could lead to

²³⁸ <https://www.mondaq.com/uk/product-liability-safety/731088/product-marking-and-labelling-in-europe>

²³⁹ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.

²⁴⁰ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.

²⁴¹ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.

²⁴² 'Evidencing The Cost Of The UK Governments Proposed Regulatory Interventions For Consumer IoT', RSM, 2020.

²⁴³ 'Evidencing The Cost Of The UK Governments Proposed Regulatory Interventions For Consumer IoT', RSM, 2020.

²⁴⁴ Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.

complacency and overconfidence in the security of their products.²⁴⁵ However, a study of security labels for consumer IoT products found that participants didn't necessarily assume that devices with a positive label were immune from hacking, on average reporting that they thought devices with a label had over a 40% chance of being hacked.²⁴⁶

380. For the reasons outlined above, the rate of behaviour change resulting from any cyber security labelling scheme would likely be less than that of food labelling and eco-labelling, at least in the short run.

²⁴⁵ DCMS, February 2020. [Government response to the Regulatory proposals for consumer Internet of Things \(IoT\) security consultation.](#)

²⁴⁶ 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/>

Annex 3 - Risks and Assumptions

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
Number of consumer connectable products	Ofcom research report ²⁴⁷ and data from Statista on the number of smartphones ²⁴⁸	Benefits not being accurately estimated. The number of devices estimated in stock is also dependent on these estimates.	Number of consumer connectable products	Sensitivity analysis has not been used for estimates between 2018-24 but sensitivity analysis has been used for the estimated growth rate in consumer connectable products from 2024
Growth rates from consumer IoT	Transforma Insights ²⁴⁹	Forecast under or overestimates the number of consumer connectable products resulting in inaccurate benefits estimation.	Number of consumer connectable products	Sensitivity analysis used around the central estimate (16.5% in the optimistic scenario and 5.5% in the worst case scenario).
Number of consumer connectable products connected to the internet is assumed to remain constant at 92%.	RSM report ²⁵⁰	Inaccurate estimation of the number of consumer connectable products within in scope would lead to inaccurate benefits	Number of consumer connectable products	Sensitivity analysis has not been used. DCMS are confident in this estimate.
Proportion of devices within each product category	RSM consumer survey ²⁵¹	Affects the benefits through the replacement rate.	Replacement rate	This estimate is based on commissioned research. Sensitivity analysis has not been used because DCMS are confident in this estimate.
The average life of products within each category	RSM consumer survey; YouGov	Affects the benefits through the replacement rate.	Replacement rate	Varies by product group see Table 4 for details.
Distribution of replacement across the years	Data on device ownership only goes back to 2015 so for the proportion of consumers who reported owning a device before 2015 the replacement rate has been assumed to be evenly distributed across the years.	Affects the benefits through the replacement rate.	Replacement rate	Sensitivity analysis has not been used here. DCMS view this as a reasonable assumption given the lack of available evidence.
The likelihood of a cyber attack	The likelihood of a cyber attack resulting from insecure consumer connectable products has been	Inaccurately estimating the benefits.	Estimating the cost of cyber attacks	This is a best estimate given the available data. The use of this estimate has been supported by NCSC.

²⁴⁷ https://www.ofcom.org.uk/_data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf

²⁴⁸ <https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/>

²⁴⁹ <https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030>

²⁵⁰ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf

²⁵¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
	<p>estimated at 4.4%. This is a proxy and based on the number of cyber crime incidents in 2019 as a proportion of consumer connectable products in 2019.</p> <p>The estimated number of cyber incidents is based on the Crime Survey for England and Wales. The number of consumer connectable products has been estimated using two data sources (see the first assumption within the annex for details).</p>			The high estimate is 8.8%.
The probability of a cyber incident having a financial impact is assumed to be 55% and remains constant throughout the appraisal period (for consumers).	This is based on the proportion of cyber incidents that were reported as having an impact according to the Crime Survey for England and Wales.	Inaccurately estimating the benefits	Estimating the cost of cyber attacks	Sensitivity analysis has not been used here. DCMS views this as a reasonable proxy.
The unit cost of cyber crime (to consumers)	£281.55 (2019 prices) - based on Home office analysis.	Inaccurately estimating the benefits	Estimating the cost of cyber attacks	Sensitivity analysis has not been used here. This estimate is based on the best available evidence.
The reduction in the probability of a consumer falling victim to a cyber attack as a result of government intervention	Best estimate is 50%	Inaccurately estimating the benefits	Benefits	20% Worst case estimate and 80% in the optimistic estimate
The proportion of businesses that are users of consumer connectable products	Best estimate 18%.	Inaccurately estimating the benefits	Benefits	9% in the worst case scenario estimate and 26% in the optimistic scenario.
The estimated cost of a cyber attack (to a business)	Best estimate £1,010 per incident ²⁵² based on the Cyber Breaches Survey	Inaccurately estimating the benefits	Benefits	Sensitivity analysis has not been used here. DCMS are confident in this estimate.
The probability of a cyber attack having a financial impact	Best estimate 46% - based on Cyber Security Breaches Survey, 2020.	Inaccurately estimating the benefits	Benefits	Sensitivity analysis has not been used here. DCMS are confident in this estimate.
Assumed that benefits will not accrue in year 1 but that costs will.	Based on a conservative approach to estimating benefits	The risk is that the benefits in year 1 will be undervalued.	Benefits	Sensitivity analysis has not been used here. This decision is

²⁵² Cyber Security Breaches Survey 2020

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
				based on a conservative approach to estimating benefits.
Benefits of a more secure device will be cumulative (i.e consumers will continue to benefit for as long as the device is still is use)	The estimates in Table 5 have been used to determine the average life of different product groups.	Overestimating the benefits	Benefits	Sensitivity analysis is not applicable here.
The proportion of devices sold with a 'positive label' under the voluntary labelling scheme scenario.	In the central and optimistic scenario the estimate is 1.8%. This is based on the number of businesses (3) that have publicly committed their adoption of the security requirements set out in the code of practise, as a proportion of UK manufacturers (170). In the worst case scenario the estimate is 0.27%.	Inaccurately estimating the benefits	Benefits	In the central and optimistic scenario the estimate is 1.8% and in the worst case scenario the estimate is 0.27%.
The proportion of consumers that switch to a device with a 'positive label' under the voluntary labelling scheme scenario.	Based on evidence from food labelling schemes.	Inaccurately estimating the benefits	Benefits	Sensitivity analysis has been used around the central estimate. 10% in the worst case scenario and rising gradually. 51% in the optimistic scenario.
The proportion of devices sold with a 'positive label' under the mandatory labelling scheme scenario.	A DCMS assumption.	Inaccurately estimating the benefits	Benefits	Sensitivity analysis has been used and ranges from 13% in the worst case scenario to 50% in year 2, rising to 90% in the optimistic scenario.
The proportion of consumers that switch to a device with a 'positive label' under the mandatory labelling scheme scenario.	Based on evidence from food labelling schemes.	Inaccurately estimating the benefits	Benefits	Sensitivity analysis has been used around the central estimate. 13% in the worst case scenario and 51% in the optimistic scenario.
The number of manufacturers and retailers in scope	The best estimate is 170 ²⁵³ manufacturers and 3,485 ²⁵⁴ .	Inaccurately estimating the cost of intervention	The number of manufacturers and retailers in scope	Sensitivity analysis has been used. In the central and the optimistic scenario the estimated number of retailers within scope is 3,485 but this rises to 3,675 in the worst case scenario. The

²⁵³ RSM survey, Evidencing the cost of the UK governments proposed regulatory interventions for consumer IoT, 2020.

²⁵⁴ <https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/>

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
				number of retailers within scope is 170 in the central and worst case scenario but falls to 69 in the optimistic scenario.
Time spent on familiarisation	RSM business survey ²⁵⁵	Inaccurately estimating familiarisation costs	Familiarisation costs	This is based on commissioned evidence. Sensitivity analysis has not been used here. DCMS are confident in this estimate
Average wages	RSM business survey ²⁵⁶	Inaccurately estimating both self-assessment and familiarisation costs	Familiarisation costs and self-assessment costs	Sensitivity analysis has not been used here. DCMS are confident in this estimate.
Time spent on self-assessment	RSM business survey ²⁵⁷	Incorrectly estimating the self-assessment costs	Self-assessment costs	Sensitivity analysis has not been used here. DCMS are confident in this estimate.
The average number of product lines	RSM business survey	Incorrectly estimating the labelling costs	Labelling costs	Sensitivity analysis has been used here. The average number of product lines varies from 8 in the optimistic and central estimate to 21 in the worst case scenario.
The average cost of changing a product line per manufacturer	£3000 (£2010 prices)	Incorrectly estimating the labelling costs	Labelling costs	
Average cost of implementing security requirement 1 (default passwords)	The average cost of implementing Security requirement 2 and Security requirement 3 was used as a proxy for Security requirement 11 due to a lack of available evidence. Evidence from the RSM business survey, 2020.	Incorrectly estimating the security improvements	Security Improvements	Costs associated with implementing the security requirements have been varied by 20% around the central estimate.
Under the mandatory labelling scheme scenario it has been	This is based on the estimated proportion of consumer	Overestimate the costs	Disposal of non-compliant stock	Sensitivity analysis has been used here. 10% is the central

255

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things_IIoT_products.pdf

256

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things_IIoT_products.pdf

257

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things_IIoT_products.pdf

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
assumed that 10% will be disposed of.	connectable products in the UK with 'default passwords'.			estimate, 5% is the optimistic estimate and 45% is the worst case scenario.
Under the top 3 (policy option C) scenario it has been assumed that 10% stock will be disposed of.	Compliance data based on 253 Which? Investigations.	Overestimate the costs	Disposal of non-compliant stock	Sensitivity analysis has not been used here. The 10% assumption is considered an overestimate but a conservative approach has been taken due to a lack of available evidence.
Average retail turnover	Inventory retail turnover from Walmart, 2019 Statista.	Does not represent the average retailer of consumer connectable products in the UK	Disposal of non-compliant stock	Sensitivity analysis has not been used here. This is considered a good proxy for retailers of consumer connectable products
The value of consumer connectable products	RSM consumer survey, 2020	Incorrect cost estimates	Disposal of non-compliant stock	DCMS are confident in this central estimate. Sensitivity analysis has not been used.
The direct cost of disposal per device	RSM survey, 2020	Incorrect cost estimates	Disposal of non-compliant stock	DCMS are confident in this central estimate. Sensitivity analysis has not been used.