Title: Regulation of consumer connectable product cyber security	**Impact Assessment (IA)**
	Date: 10 July 2023
IA No:	**Stage:** Final
RPC Reference No: RPC-DCMS-4353(4)	**Source of intervention:** Domestic
Lead department or agency: Department for Science, Innovation and Technology (DSIT)	**Type of measure:** Secondary legislation
Other departments or agencies: National Cyber Security Centre (NCSC)	**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**
£-193.2m	***£-187.3m***	***£21.8m***	**Qualifying Provision**

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

Parliament recently enacted the Product Security and Telecommunications Infrastructure Act 2022 ("the PSTI Act") which empowers the Secretary of State to specify security requirements that must be complied with in relation to consumer connectable products made available to customers in the United Kingdom. Many of these products contain vulnerabilities that not only pose a serious threat to individual privacy and security, but 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[1] and international standards[2]. Too many insecure consumer connectable products remain on the market and we need to take steps to ensure that in future, these products can be used 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. The government has now prepared Regulations ("The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023" or "the instrument" / "the Regulations"), that will enable the product security regime established by the PSTI Act to be implemented.

[1] DCMS, 2018. *Code of Practice for Consumer IoT Security*
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[2] European Telecommunications Standards Institute, 2020, *Cyber Security for Consumer Internet of Things: Baseline Requirements*
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

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 relating to 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[3] that was published in 2018 has been adopted by many countries across the world and has influenced the development of international standards. DSIT 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 1:** Voluntary labelling scheme
- **Option 2:** Mandatory labelling scheme
- **Option 3 (preferred legislative option):** Bring the PSTI product security regime into force to ensure that **all** consumer connectable products made available to UK customers comply with a minimum security baseline, initially based on 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: 06/07/2023

[3] DCMS, 2018. *Code of Practice for Consumer IoT Security*
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

Summary: Analysis & Evidence - Policy Option 1

Description: The government introduces a voluntary security label for use by manufacturers of consumer connectable products. This will address the information asymmetry market failure by making clear to consumers whether a product complies with a minimum security baseline that would initially be based on 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)		
			Low:	High:	Central:
2019	2020	10	£-25.9m	£-10.4m	£-21.3m

COSTS (£M)	Total Transition (2022)		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£10.4m		£0.0m	£10.4m
High	£25.7m		£0.0m	£25.9m
Central Estimate	£21.1m		£0.0m	£21.3m

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

Transition costs include familiarisation costs associated with implementing the label, which apply to all retailers and manufacturers in scope. Ongoing costs include self-assessment costs, which only apply to manufacturers. DSIT estimates that there are 170 manufacturers in scope. In addition to this, DSIT has estimated that there are 3,485 retailers and 11,200 charity stores, which combined comprise all retailers in 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 for this subset of firms, resulting in lower profits.

BENEFITS (£M)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefits (Present Value)
Low	N/A		N/A	N/A
High	N/A	N/A	N/A	N/A
Central Estimate	N/A		N/A	N/A

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

N/A

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 experiencing a reputational benefit and 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. There is also a potential benefit to wider society of having fewer insecure consumer connectable products in the market, and fewer sales of these products, which are open to hacking and use in wide-scale Distributed Denial of Service (DDoS) attacks, albeit this benefit will be greater in the other options.

Key assumptions/ sensitivities / risks	**Discount rate (%)**	3.5%

1. DSIT assumes that the adoption of the voluntary label will occur gradually, as manufacturers incorporate the label into their business as usual updates to their packaging (in order to minimise their costs). Therefore, DSIT assumes that there are no additional costs associated with adding the voluntary label to packaging.
2. DSIT assumes 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, DSIT assumes that only 0.39% of new products are purchased with a positive label throughout the appraisal period, which is based on the estimated probability of a product meeting 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 increasing by 1% per year throughout the appraisal period to 19% in year 10. This is based on food labelling research.
4. DSIT estimates 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 1)

Direct Impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	
£2.5m	£0.0m	£2.5m	£12.3m

Summary: Analysis & Evidence - Policy Option 2

Description: Mandate retailers to only sell consumer connectable products that have a security label indicating whether or not the product meets a minimum security baseline, that would initially be based on 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	PV Base Year	Time Period (Years)	Net Benefit (Present Value (PV)) (£m)		
2019	2020	10	**Low :** £-156.1m	**High:** £-60.7m	**Central Estimate:** £-129.5m

COSTS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£54.1m		£0.8m	£60.7m
High	£137.8m		£2.1m	£156.1m
Central Estimate	£114.5m		£1.8m	£129.5m

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

Transition costs include familiarisation costs; labelling costs and 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 affect both retailers and manufacturers. Ongoing costs include self-assessment costs and only affect manufacturers. DSIT estimates that there are 170 manufacturers in scope. In addition to this, DSIT estimates 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 bearing a "negative" label would likely incur reputational damage, which could result in lower sales resulting in 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	N/A		N/A	N/A
High	N/A	N/A	N/A	N/A
Central Estimate	N/A		N/A	N/A

Description and scale of key monetised benefits by 'main affected groups'
N/A
Other key non-monetised benefits by 'main affected groups'
Mandating that consumer connectable products are only sold 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 baseline 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. DSIT assumes that retailers will dispose of 10% of their current stock of consumer connectable products in the central estimate. The low scenario is a 5% disposal of current stock.
4. DSIT estimates 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.
6. DSIT assumes that the number of businesses will grow by 3% per annum.

BUSINESS ASSESSMENT (Option 2)

Direct Impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	
£14.4m	£0.0m	£14.4m	£71.8m

Summary: Analysis & Evidence - Policy Option 3

Description: Bring the PSTI product security regime into force to mandate a minimum security baseline for consumer connectable products, with this baseline initially based on the top three guidelines of the Code of Practice.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period (Years)	Net Benefit (Present Value (PV)) (£m)		
2019	2020	10	**Low :** £-222.0m	**High:** £-90.0m	**Central Estimate:** £-193.2m

COSTS (£M)		Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	£73.0m		£2.0	£90.0m
High	£177.0m		£5.3	£222.0m
Central Estimate	£151.8m		£4.8	£193.2m

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

Transitional costs include familiarisation costs, costs associated with the statement of compliance, as well as costs associated with the disposal of non-compliant products. The transitional costs are 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. DSIT estimates that there are 170 manufacturers in scope. In addition to this, DSIT estimates 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, DSIT expects that some products will no longer be available on the UK market due to non-compliance, which would 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	N/A	N/A	N/A	N/A
High	N/A		N/A	N/A
Central Estimate	N/A		N/A	N/A

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

N/A

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

The direct benefits to consumers from a reduction in the number of cyber crime incidents is the main benefit of this policy option. 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. DSIT assumes 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 10% of products will be disposed of, as default passwords is the only security update that may not be possible post production.
2. DSIT assumes that all 'small and micro' manufacturers pass their direct costs onto consumers. Using IoTUK data, DSIT estimates that 72% of manufacturers are 'small' and 98% of retailers are either 'small' or 'micro' businesses.
3. In the central scenario, DSIT assumes that mandating the initial minimum security baseline leads to a 50% reduction in the number of cyber crime incidents.
4. DSIT estimates 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.
6. DSIT assumes that the number of businesses will grow by 3% per annum.

BUSINESS ASSESSMENT (Option 3)

Direct Impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs:	**Benefits:**	**Net:**	
£21.8m	£0.0m	£21.8m	£108.8m

Table of Contents

Section 1 - Products in scope and key terminology

1. The Product Security and Telecommunications Infrastructure Act 2022 ("the PSTI Act") was recently enacted by Parliament. DSIT has also prepared the draft The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 ("the Regulations" / "the instrument"), which the Government intends to make under the relevant powers in the PSTI Act, as well as the power in Section 8C of the European Union (Withdrawal) Act 2018. These Regulations will apply to a broad range of consumer connectable products. This includes smartphones that are made available to UK 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 PSTI product security regime. Further details of the way in which the PSTI Act defines 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 regulation

- *Smartphones, and tablets capable of connecting to cellular networks*
- *Routers and Wi-Fi access points*
- *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*
- *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 the physical connectable products made available to consumers. Other aspects will apply to both these products, and any digital services associated with the device ("associated services", such as mobile applications and cloud storage. The term "**products**" should be understood to refer to both "**devices**" (physical products) 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 regime. It should be understood as referring to internet-connectable or network-connectable product lines that are made available to consumers.

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 captures both the physical product and their associated services,, 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 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	*Physical thing (hardware) and software components*
Associated Services	*Digital services that, together with the device, are part of the overall product and that are required to provide the product's intended functionality.*
Product	*'device' and its 'associated services'*

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, or poor security practices relating to them. Citizens, networks and the wider economy are therefore 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.[4] In addition to this, there were an estimated 58 million smartphone users in the UK in 2019. This is expected to increase to 65 million by 2025.[5]

8. A 2020 survey of 3,959 consumers by Ofcom found that the most prevalent internet-connectable devices in the UK include:[6]

   - **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 into devices falls, manufacturers will continue to connect more and more devices to the internet.[7]

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.[8]

11. It is worth noting however, that not all devices which are purchased will be connected to the internet. Research by RSM reported that on average, 4% of devices were used, but not connected to the internet, while 3% were owned but not used.[9] How this is accounted for is detailed in Section 7B(i) - Estimating the total number of consumer connectable products.

[4] Ofcom, 2017. *Review of the latest developments in the Internet of Things*
https://www.ofcom.org.uk/___data/assets/pdf_file/0020/108515/connected-nations-internet-things-2017.pdf

[5] 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/. Accessed 17.10.2022.

[6] Ofcom, 2020. *Technology Tracker 2020 Data Tables*
https://www.ofcom.org.uk/___data/assets/pdf_file/0037/194878/technology-tracker-2020-uk-data-tables.pdf

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

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

[9] RSM, 2020. *Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT*
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

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

12. The overall impact of COVID-19 on consumer connectable products within the UK, and how this affected long term trends 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, during the COVID-19 pandemic from March - November 2020, six in ten consumers in the UK (57%) reported an increase in their household use of smart devices.[10] Furthermore, according to the Vodafone IoT spotlight Report 84% of businesses claimed IoT was essential for their survival during the COVID-19 pandemic[11].

13. There is also evidence that cyber attacks increased during the pandemic. According to research undertaken by Checkpoint, "71% of security professionals noticed an increase in security threats or attacks since the beginning of the pandemic".[12] Kaspersky, also reported that attacks targeting IoT devices in the first six months of 2021 doubled in comparison to the six months previous.[13] 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, and has also left them vulnerable to cyber attacks. Therefore, with evidence suggesting an 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

14. 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 measures in place, for example a vulnerability disclosure policy allowing security researchers to report vulnerabilities to the manufacturer.[14]

15. Consumers are both unaware that their connectable products are potentially insecure[15], whilst also not being provided with sufficient information about the security of these products to allow them to make an informed purchasing decision.[16] Moreover, only one in five consumers are actively taking steps to check the security provisions linked to their connectable products.[17]

16. 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.

17. 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 absence of a user interface

---

[10] Ipsos Mori. December 2020. *Consumer attitudes towards IoT Security Survey Report* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

[11] Vodafone, 2020. *IoT Spotlight Report* https://www.vodafone.com/business/news-and-insights/white-paper/iot-spotlight-2020

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

[13] Daws (2021). *Kaspersky: Attacks on IoT devices double in a year. IoT News* https://www.iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-in-a-year/

[14] *IoTSF, 2021 The contemporary Use of Vunerability Disclosure in IoT* https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf

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

[16] 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?

[17] Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

makes it harder for consumers to change default passwords or to change security settings and update their device, making them less secure.[18,19]

2D - Impact of insecure consumer connectable products on citizens

18. 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.

19. 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.[20]

20. 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.[21] A denial of service attack is defined by the National Cyber Security Centre (NCSC) as an attack where legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. These attacks can be carried out using a botnet, which is a network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.[22]

21. Alternatively, if smart locks or connectable physical access control systems are compromised, criminals could get into homes without needing to force entry.[23] 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.[24] This poses both a safety and security risk to homeowners.

22. 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.[25] 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.[26] 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 a further three which were critical vulnerabilities. Several devices could allow hackers to steal the network's password which could then be used to hack into other connectable devices.

23. 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):

---

[18] 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

[19] Default passwords are passwords that are preinstalled on a product that 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.

[20] Which? 2017. Safety alert: see how easy it is for almost anyone to hack your child's connected toys. https://www.which.co.uk/news/article/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys-a5BL72j4HeAS

[21] International Business Times, 2016, accessed at: https://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639

[22] NCSC Glossary: https://www.ncsc.gov.uk/information/ncsc-glossary

[23] 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/

[24] https://www.techradar.com/uk/news/smart-lock-security-issues-leave-the-door-open-for-hackers

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

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

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.[27,28] 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 Original Device Manufacturer (ODM) 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.[29,30] 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 regime 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.

24. Furthermore, during the COVID-19 pandemic from March-November 2020, six in ten consumers in the UK (57%) reported an increase in their household use of smart devices.[31] 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 45% of businesses and 64% of charities reporting that staff in their organisation regularly use their own device or Bring Your Own Device (BYOD), it is important that consumers and their employers know whether products use for work will receive security updates.[32]

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

25. 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 knowledge[33]) could affect essential systems such as electricity supplies and power grids.[34]

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.[35] 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).

[27] https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/
[28] https://www.pentestpartners.com/security-blog/tracking-and-snooping-on-a-million-kids/
[29] https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/
[30] *https://www.bbc.co.uk/news/technology-51751950*
[31] Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.
[32] Cyber breaches survey 2022.
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
[33] NCSC Glossary: https://www.ncsc.gov.uk/information/ncsc-glossary
[34] 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
[35] https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

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 Domain Name System (DNS) provider Dyn.[36] Post-incident analysis by Dyn[37] 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.[38] Since then, Mirai botnets have been used to attack Liberian internet exchanges[39], and UK banks including Lloyds and RBS[40] leading to disruption to customers.

Research by Which? using a honeypot 'smart home' determined that 97% of attacks against smart devices are seeking to add them to the Mirai botnet.[41]

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. [42] 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 address[43], with over 40 thousand based in the UK[44] – 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 in 2016.

26. Researchers at the University of California sought to determine the cost to consumers of insecure Internet of Things devices[45] 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 be incurred by the owners of devices taken control of by hackers when used in these attack scenarios.[46] Information on the limitations of this study are noted below.

27. 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 was a key guideline of the also advocated by guideline one of the UK government's 2018 Code of Practice for IoT Security (see 3D - Previous UK government Interventions for further details), and a requirement of the PSTI product security regime.

    - 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.

[36] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[37] https://web.archive.org/web/20161107182254/http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[38] https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/
[39] https://grahamcluley.com/did-mirai-botnet-liberia-offline/
[40] https://www.bbc.co.uk/news/business-38715909
[41] Which? 2021. How a smart home could be at risk from hackers.
[42] https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173/
[43] https://viz.greynoise.io/query/?gnql=tags%3A%22Mirai%22
[44] https://viz.greynoise.io/query/?gnql=tags%3A%22Mirai%22%20country%3A%22United%20Kingdom%22
[45] https://groups.ischool.berkeley.edu/riot/
[46] 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.

- 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.

28. Since this work was conducted several years ago it is worth noting that the potential size and impact of such attacks have increased, with examples of attacks delivering 46 million requests per second[47]. For comparison, the KrebsOnSecurity attack used as part of this analysis generated 450,000 requests per second. In addition the cost of energy has substantially increased since the research was conducted suggesting that a worst-case attack today would likely cost consumers considerably more.

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

Attack	Cost
Scenario 1: Krebs On Security Attack[48] 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.	According to their cost calculator, the total electricity and bandwidth consumption costs borne by consumers in this attack was $323,973.75.
Scenario 2: The Dyn, Inc. Attack 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.[49] 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.	Total electricity and bandwidth consumption costs borne by consumers as $115,307.91.
Scenario 3: "Worst-Case" Attack. This hypothetical “Worst-Case” scenario approximates the costs that could result if the Mirai botnet operated at its peak power.	The projected total electricity and bandwidth consumption costs to consumers of this attack is $68,146,558.13.

29. Research by BitSight found that around 8% of web domains which relied on Dyn’s services stopped using their services after the attack.[50] This demonstrates that cyber security can have a real commercial impact on businesses.

30. 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,

[47] ITPro, 2022. Record for the largest ever HTTPS DDoS attack smashed again. https://www.itpro.co.uk/infrastructure/network-internet/368857/record-for-largest-ever-https-ddos-attack-smashed-again
[48] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[49] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
[50] https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/

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.

31. 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[51] in the UK and the attacks that caused disruption to internet access in Liberia.[52]

32. As networks of hijacked computer devices, botnets can also be used for a range of malicious purposes beyond DoS attacks.[53] Botnets can be used in phishing schemes sending out malicious emails in order to steal information such as users' passwords, in cryptocurrency scams using the the hijacked device's processing power to mine for cryptocurrency, and in brute force attacks using the processing power of its devices to gain unauthorised access to another system by trying different password combinations.

33. The use of botnets that incorporate consumer connectable devices in these types of attacks demonstrates that poor cyber security can lead to the proliferation of further cyber attacks that could impact both individuals and businesses.

2F - Impact of insecure consumer connectable products on businesses

34. 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, 36 organisations provided responses on their organisations relationship with consumer IoT with 28% reporting that they used consumer IoT devices.[54]

35. A 2018 survey predicted that IoT would become important for 92% of businesses in 2020.[55] 50% of 950 companies surveyed globally in 2018 reported using IoT devices made by a third party, and 33% used their own IoT devices.[56] However only 42% of UK respondents reported that their organisations were able to detect when any of their IoT devices had been breached.[57]

36. Moreover, research in 2019 found that 49% of UK businesses had unknown devices on their network.[58] 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.[59]

37. Statistics from 2018 highlight that in the UK, 45% of businesses allowed staff to use personally-owned devices for regular work.[60] In addition the cyber security breaches survey revealed that 50% of businesses with cyber security policies, have staff that use personally owned devices, such as laptops, to carry out work-related activities.[61] For charities, this figure was 53%. 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.

38. 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,

[51] https://www.bbc.co.uk/news/business-38715909
[52] https://grahamcluley.com/did-mirai-botnet-liberia-offline/
[53] https://www.kaspersky.co.uk/resource-center/threats/botnet-attacks
[54] 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.
[55] 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
[56] Gemalto, 2018. State of IoT Security Report. https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf
[57] Gemalto, 2018. State of IoT Security Report. https://www.infopoint-security.de/media/gemalto-state-of-iot-security-report.pdf
[58] https://www.information-age.com/uk-businesses-iot-ot-cyber-attacks-123479373/
[59] https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/
[60] Statista. 2020. Share of United Kingdom (UK) business where bringing your own device occurs in 2018
[61] Cyber Security Breaches Survey 2023.

with the remaining 83% of IoT-based transactions using plain text channels, exposing this traffic to a range of exploits.[62]

39. The 2023 Cyber Security Breaches Survey found that among businesses identifying any breaches or attacks, the average cost of the most disruptive breach was approximately £1,100[63]. The estimate for medium and large businesses was £4,960.. Although the breaches in this survey may not have been caused by insecure consumer connectable products, this demonstrates that cyber attacks against organisations can potentially have a significant financial impact.

40.

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.[64]

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

41. 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.

42. 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.

43. 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.[65] 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.

Section 3 - Rationale for intervention

44. 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 consumer connectable products sold across the UK will meet essential cyber security standards

[62] Zscaler (2022). https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022.
[63] Cyber Security Breaches Survey 2023
[64] 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/
[65] 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

45. 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 measures in place, despite the publication of best practice guidance. This leaves networks and infrastructure, consumers, and businesses vulnerable to the impacts of cyber security breaches.

46. 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.

47. The 2022 Impact Assessment for the PSTI product security regime presented three distinct market failures as the rationale for intervention, which were externalities, information asymmetry and misaligned incentives. Upon reflection, DSIT believes that the misaligned incentives are a product of the information asymmetry and externalities. This means that there are only two rationales for intervention in this impact assessment.

3A - Externalities

48. 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.

49. The costs of cyber attacks enabled by insecure consumer connectable products are often 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 exploited.[66,67] Therefore, fewer insecure products connected to the internet (or connected to products that connect to the internet) would reduce the risk of cyber attacks (including wide scale botnet attacks) enabled by vulnerabilities in these products, leading to a safer UK network for all consumers and businesses. Further details on botnet attacks are provided in the preceding section 2E - Botnets, and the impact of insecure consumer connectable products on networks and infrastructure.

50. 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

51. 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.

52. Research suggests that there is currently a significant lack of information provided to consumers on the built-in security provisions for connectable products.[68] 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.[69,70]

53. Moreover, 72% of consumers believe that security features are already built into the devices they buy.[71] This indicates that many consumers are unaware of the security standards in consumer connectable

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

[67] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#preventmalwaredelivery

[68] Blythe, J. M., Sombatruang, 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/

[69] Ipsos Mori. December 2020. Consumer attitudes towards IoT Security Survey Report.

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

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

products. Consequently, consumers are not able to demand a higher level of security from manufacturers of these products.

54. 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 ostensibly 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 - 2E - 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.

55. As a result of this information asymmetry, consumers are unable to access the information needed to inform their purchasing decisions. e. The result of this is that when purchasing connectable products, consumers may unwittingly be putting themselves at an increased risk of cyber attack.

3C - Summary of Market Failures

56. 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 are unable to access the information, and may lack the knowledge, to be able 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 section 3E - Prevalence of baseline security measures for further details).

3D - Previous UK Government Interventions

57. 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"[72] (see Box 7 for further details).

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."

58. 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.

59. 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.[73] This report was developed through extensive engagement with industry and subject matter experts.

60. The Government's preference has always been for the market to be able to solve the problems presented by insecure consumer connectable products without government intervention. 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.

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

[73] https://www.gov.uk/government/publications/secure-by-design-report

61. 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.[74] The thirteen outcome-led guidelines featured in the Code of Practice are detailed in Box 8.

62. 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

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

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

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."

63. 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.

64. DSIT 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[75], setting our security provisions for consumer internet of things devices. The standard was published in June 2020 , building upon the Technical Specification published by ETSI in February 2019[76].

65. During the passage of the PSTI Act through Parliament the UK government published the National Cyber Strategy 2022[77], with further details set out inBox 9 below. This impact assessment relates to the PSTI product security regime that seeks to meet objective 3 under pillar 1 of this strategy.

Box 9 - National Cyber Strategy (2022)

Pillar 1- Objective 3:

Secure the next generation of connected technologies, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply

Under this objective, the strategy states that by 2025 the UK will have achieved the following outcome:

"Consumer connectable products sold across the UK meet essential cyber security standards."

66. 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.

3E - Prevalence of baseline security measures

67. 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.[78] Only three manufacturers of consumer connectable products have publicly pledged to the Code since it was first launched.[79] 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).

68. 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

[75] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
[76] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
[77] UK National Cyber Strategy 2022.
https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[78] https://cyber-itl.org/2019/08/26/iot-data-writeup.html
[79]
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

than this evidence implies, as although some manufacturers may no longer produce devices with universal 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 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.

69. 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 whether their product was ever, or if it is still, 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.[80]

3E(i) - Progress in eliminating Universal Default Passwords

70. 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 following the publication of the 2018 Code of Practice, (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.

71. Other research suggests, based on a sample of 270 devices, that at least 4.7% of devices on the market contain a default password.[81] 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.[82]
- 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.

72. Given the Mirai botnet was able to launch large-scale attacks using a botnet comprising as few as 145,000 devices[83], the estimated prevalence of default passwords in consumer connectable products continues to leave open the risk of an attack of this nature recurring.

73. Despite the introduction of the voluntary Code of Practice, somewhere between one in ten and one in twenty devices still potentially have a universal default password. This would indicate that the voluntary Code of Practice was not sufficiently effective in eliminating this vulnerability..

74. In addition to this, a recent (late 2020) Ipsos MORI survey commissioned by the department 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 having a limited impact on user behaviour. This highlights the need for regulation so that responsibility for improving the security of products is taken away from consumers.[84]

---

[80] Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019

[81] 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? 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.

[82] 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? https://osf.io/preprints/socarxiv/63zkt/

[83] https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations#:~:text=Mirai's%20attack%20peaked%20at%20an,attack%20peaking%20around%20400%20Gbps.

[84] 'Attitudes Towards IoT security', Ipsos Mori.

3E(ii) - Prevalence of Vulnerability Disclosure Policies

75. Although work has previously been undertaken to develop best practices for vulnerability disclosure through voluntary International Standards Organization (ISO) standards,[85] evidence suggests that a significant amount of consumer connectable product manufacturers have not fully embraced the principles underlying coordinated vulnerability disclosure.

76. The Internet of Things Security Foundation has conducted a series of annual research reports that 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).[86] In 2020 this had increased to 18.9% of those surveyed having a vulnerability disclosure policy, which had further increased to 21.6% in 2021[87]. In the 2022 sample, this figure had increased to 27.1%.[88] Although this research shows improvements over time, it also demonstrates that a significant majority of global manufacturers still do not have robust systems in place to enable the reporting of identified vulnerabilities. This suggests that the Voluntary Code of Practice may have led to improvements in this space, albeit at a slow pace.

77. The Vulnerability disclosure policy, and its implementation, is the route for 'anyone' to report issues, bugs, breaches, problems etc to a manufacturer, or a party acting on their behalf, so they are able to resolve or mitigate the issue. This means that the majority of manufacturers do not provide a clear route for security issues affecting their products to be reported to them, resulting in vulnerabilities remaining unresolved and open to exploitation. According to the statistics quoted above, this equates to 240 manufactures, making multiple product lines, of which there may be hundreds or thousands of individual products that may be more vulnerable as a result.

78. The absence of mechanisms by which vulnerabilities can be reported to manufacturers limits 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 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.

3E(iii) - Prevalence of timely software updates, and transparency on how long products will receive security updates for

79. 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.

80. 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.[89] 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.

81. 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.[90]

82. 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

[85] 6 ISO/IEC 291471 and ISO/IEC 301112 https://www.iso.org/home.html

[86] IoTSF. 2020. Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report. https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf

[87] Copper Horse. The state of Vulnerability Disclosure policy (VDP) usage in Global Consumer IoT in 2022

[88] Copper Horse. The state of Vulnerability Disclosure policy (VDP) usage in Global Consumer IoT in 2022

[89] 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? https://osf.io/preprints/socarxiv/63zkt/

[90] https://www.which.co.uk/news/2020/03/more-than-one-billion-android-devices-at-risk-of-malware-threats/

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.[91]

3E(iv) - Summary of baseline security measure prevalence

83. Whilst compliance with the top three Code of Practice guidelines has seen some limited improvement, the available evidence convincingly suggests that voluntary regulation has not been sufficient to ensure the implementation of basic security measures to protect consumers using connectable products... Default passwords are still prevalent in 10% of devices. Only 27.1% of manufacturers provide clear routes for vulnerabilities affecting their products to be reported to them.. Based on the data available to the Internet of Things Security Foundation as of their January 2023 research report, they estimate that 100% of surveyed manufacturers would not have vulnerability disclosure policies in place until 2039[92]. Additionally, there is a continued absence of clear accessible information on whether a product will be supported with security updates, or how long it will be supported for. This makes it clear that the market failure of asymmetric information continues to prevent consumers from making purchasing decisions informed by the additional security risks they may expose themselves to when selecting a particular product.

3F - What sectors / markets / stakeholders will be affected, and how, if the government does intervene?

3F(i) - Impact on the manufacturers and retailers

84. For the purposes of the cost-benefit analysis in this impact assessment, DSIT has identified 170 UK manufacturers and 3,485 retailers that will be directly affected by the PSTI product security regime.[93] The regime places proportionate duties on 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 implement a minimum security baseline relating 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.[94] The introduction of this regime 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 initial minimum security baseline; costs associated with creating a statement of compliance; as well as costs resulting from the disposal of non-compliant goods.

3F(ii) - Impact on the cyber security insurance market

85. Another sector that may be impacted by the PSTI product security regime is the cyber insurance sector. The personal cyber insurance market offers protection against a wide range of harms, including cyber extortion, cyber bullying, online fraud and data breach, with at least one company offering plans r that cover the cost to restore smart devices and wearables affected by a cyber attack.[95] The UK Insurance Consumer Survey 2020 found that 1 in 5 individuals were interested in purchasing a cyber insurance policy, although overall, the Department has found limited evidence concerning the size of the UK personal cyber insurance sector, and no evidence of a significant market for personal insurance plans focused on (or UK insurers specialising in) connectable product security.

86. As it is possible that the PSTI product security regime could impact consumer perceptions about the security risks associated with connectable products, the implementation of the regime could therefore indirectly affect the personal cyber insurance market. Enhanced consumer awareness of the cyber risks associated with their products could result in more UK consumers taking out personal cyber insurance policies. Whilst it is also possible that the implementation of mandatory security protections could

[91] https://www.which.co.uk/news/2020/06/the-truth-behind-smart-appliance-security-updates/
[92] Copper Horse. The state of Vulnerability Disclosure policy (VDP) usage in Global Consumer IoT in 2022
[93] https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/
[94] https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/
[95] NFU Mutual. Personal cyber cover.

disincentivize potential customers from extending or taking out new policies, owing to a perception that new devices purchased will be reliably secure, as research suggests that 72% of UK citizens understood devices on the market to be appropriately secure prior to the regime's implementation. The Department's assessment of the available evidence suggests that it is unlikely the volume of existing security-conscious policy holders sufficiently reassured by the regime's protections to exit the market, would exceed the volume of market entrants newly aware of cyber risks, including those associated with existing devices purchased before the regime came into force.

87. It should be noted that whilst the objective of the initial security baseline mandated by the PSTI product security regime is to reduce the risk of consumer connectable products being compromised by malicious actors, some risk will remain, and so the regime's introduction would not remove the benefits offered by personal cyber insurance plans to consumers looking to minimise their personal exposure to the impact of cyber crime. It is also possible that this regime may stimulate the insurance market by clarifying a measurable standard of security, which could be used as the basis for the development of new insurance products. Additionally, the provisions of this regime will have limited to no impact on most of the perils covered by existing personal cyber insurance policies, such as personal data being included in a third party data breach, or cyber harassment. security baseline

88. We also note that many of the key business lines that make up the overall UK insurance sector relate to perils that are also the subject of UK consumer protection legislation. Car safety has been subject to some degree of regulation in the UK since 1861[96], but this did not prevent the emergence of the first car insurance policies in the late 1800's[97]. The safety of contemporary cars on UK roads is now subject to an extensive regulatory framework, but motor insurance still represented over half of the UK General Insurance Market in 2022[98], with most drivers opting for motor insurance plans that go beyond the minimum mandated in law[99,100].

89. Additionally, some personal cyber insurance products are now included as part of standard home insurance cover. Given that individuals may not be actively selecting personal cyber cover but purchasing this as part of another insurance product[101], and that individuals who do have concerns regarding their personal cyber risk will still likely face cyber threats, alongside the other factors set out in this section, the Department considers it to be unlikely that the PSTI product security regime will have a significant impact on this sector.

[96] Locomotive Act 1861 - https://www.legislation.gov.uk/ukpga/Vict/24-25/70/enacted
[97] Swiss Re - A History of UK Insurance
[98] GlobalData - United Kingdom (UK) General Insurance Market Size and Trends by Line of Business, Distribution Channel, Competitive Landscape and Forecast, 2023-2027
[99] Guardian - Third-party insurance holders pay more money for less cover - 31 October 2015
[100] GoShorty - 20 UK Car Insurance Statistics You Should Know - 18 October 2022
[101] NFU Mutual. Personal cyber cover.

Section 4 - Policy objective

90. 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 in and inadequate security measures relating to 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.
    - *Since publishing the Code of Practice, our work has been amplified by the Five Eyes Community (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.*[102]
    - *The UK and India signed the India-UK cyber statement in April 2022, which included a commitment to work closely together to ensure IoT devices are secure by design.*[103]
    - *Through the Agile Nations Network, the UK, Singapore and Canada published a joint statement of intent to work together to encourage international alignment and adoption of international standards to improve the security of IoT devices.*[104]
    - *Governments of Australia (2020)*[105] *and India (2021) have published Codes of Practice with the same thirteen principles as those we published in 2018.*[106]
    - *EN 303 645 is the world's first international standard for consumer IoT. It was based on the Code of Practice and was developed at the European Telecommunications Standards Institute (ETSI). 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 DSIT. The Radio Equipment Directive Delegated Act 2022/30 is expected to develop harmonised european standards (HENs) that where appropriate draw on EN 303 645 in relation to consumer IoT.*
    - *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 Agency.*[107]
    - *We worked 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.*
    - *The Atlantic Council think tank produced a report looking into different international approaches to protecting IoT, with the UK held up as an example due to the maturity of our*

[102] Home Office, 2019. Statement of Intent regarding the security of the Internet of Things. https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

[103] Prime Minister's Office, 2022. India-UK cyber statement, April 2022. https://www.gov.uk/government/publications/prime-minister-boris-johnsons-visit-to-india-april-2022-uk-india-joint-statements/india-uk-cyber-statement-april-2022

[104] Gov.uk, 2022. Joint statement of intent from the Agile Nations working group on cyber security for consumer connected products. https://www.gov.uk/government/news/joint-statement-of-intent-from-the-for-agile-nations-working-group-on-cyber-security-for-consumer-connected-products

[105] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

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

[107] https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement

IoT cyber security approach.[108]

- *The World Economic Forum (WEF) released a joint statement of support on IoT device security which highlighted ETSI EN 303 645 as an appropriate international standard and was endorsed by 113 organisations, including DSIT.*[109]

91. 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 - adding further to the case for action.

92. As referenced in the preceding section - 3D - Previous UK Government Interventions - this work sits as part of a broader project that the Government has undertaken since the Secure by Design review[110] was first launched in December 2018. This work has been taken forward due to a specific objective in the Government's National Cyber Security Strategy (2016 - 2021), which outlines the Government's cyber security ambition over a five year period[111] and the Government's National Cyber Strategy 2022.[112] It also builds on the existing NCSC technical guidance to industry published in May 2017.[113]

93. The policy objective underpinning this regime is to protect citizens from the range of harms that can result from inadequately secure consumer connectable products. To achieve this, the regime's initial security baseline will:

- address the information asymmetry between consumers and manufacturers, incentivising manufacturers to match the security expectations of their customers through market forces.
- Ensure that manufacturers maintain an active awareness of emerging security issues affecting their products
- Ban outdated default password generation mechanisms that not only expose users to heightened individual risk of cyber attack, but could also allow malicious actors to readily access enough computing power to cause significant harm to citizens, networks, businesses, key infrastructure, and nation states. .

94. Alongside full compliance with the three security requirements that comprise the initial security baseline, DSIT aims for all UK customers purchasing consumer connectable products to be able to review the security update support period for the product, and a significant increase in the proportion of consumers that take product security into consideration when making purchasing decisions.

95. 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 baseline cyber security requirements are complied with in relation to all new consumer connectable products supplied to customers in the UK.

[108] Atlantic Council, 2022. Security in the billions.: Toward a multinational strategy to better secure the IoT ecosystem. https://www.atlanticcouncil.org/in-depth-research-reports/report/security-in-the-billions/#UK

[109] https://cybertechaccord.org/industry-hackers-and-consumers-for-a-global-baseline-for-consumer-iot-security/

[110] DCMS, 2018. Secure by Design report. https://www.gov.uk/government/publications/secure-by-design-report

[111] 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

[112] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-1-uk-cyber-ecosystem

[113] 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

96. 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 1 -** Voluntary security labelling scheme (Do-minimum option)
- **Option 2 -** Mandatory security labelling scheme (Other viable option)
- **Option 3 -** Legislating to ensure that a minimum security baseline is complied with in relation to consumer connectable products made available to UK customers, with that baseline initially based on the top three guidelines set out in the Code of Practice for Consumer IoT Security (Preferred option)

97. 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.

98. DSIT analysed the impacts of these shortlisted options as part of the process for developing the PSTI product security regime. The PSTI Act 2022 received Royal Assent in November of that year, and is due to come into effect on 29 April 2024, alongside the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023. This impact assessment expands upon the initial impact assessment for this regime[114], now that the detailed wording of the PSTI Regulations 2023 has been developed.

99. Our rationale to justify the level of analysis used in this impact assessment can be found in Section 6 - Proportionality approach.

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

100. 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. This would involve not making use of powers in the PSTI Act to introduce security requirements.

101. It should be noted that, in contrast to the consultation stage impact assessment published in 2019[115] for this work, this baseline scenario is separated from the scenario in which the government would introduce a voluntary labelling scheme (Option 1), to enable an assessment of the impacts of this non-legislative option relative to the shortlisted legislative interventions (Options 2 and 3).

102. If nothing is done, the Department would need to consider whether activity by the EU might impact Northern Ireland by way of the Northern Ireland Ireland Protocol, leaving different parts of the UK with different security requirements for consumer connected products. The EU Commission adopted the Radio Equipment Directive (RED) Delegated Act on 29 October 2021. This Act aims to make sure that wireless devices have measures to:[116]

- Improve network resilience: radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

[114] Parliament.uk, 2021. Regulation of consumer connectable product cyber security: Impact Assessment RPC-DCMS-4353(2). https://bills.parliament.uk/publications/43916/documents/1025

[115] DCMS, 2019. Mandating security requirements for consumer IoT products: Consultation Stage imapct assessment. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950420/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment_V2.pdf

[116] https://single-market-economy.ec.europa.eu/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en

- Better protect consumer's privacy: radio equipment incorporates safeguards to ensure that the personal data and privacy of the subscriber are protected.
- Reduce the risk of monetary fraud: radio equipment supports certain features ensuring protection from fraud when making electronic payments.

103. The Delegated Act will be directly applicable in Northern Ireland under Article 5(4) of the Windsor Framework[117]. Should it come into force,the Delegated Act would mandate the adoption of security measures in relation to radio equipment that would also fall in scope of the PSTI product security regime, Doing nothing would therefore leave citizens and businesses in Great Britain with fewer protections from the harms resulting from inadequately secure consumer connectable products than those in Northern Ireland..

104. On 15 September 2022 the European Commission presented a proposal for a new Cyber Resilience Act (CRA)[118] which will introduce mandatory cybersecurity requirements for products with digital elements. The cyber security regime established by the CRA will not apply in the UK, is unlikely to come into effect in the next few years, and is not currently clear what the standards enforced by it would be.

5A(ii) - Option 1 - Voluntary Security Labelling Scheme

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

106. 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 based on the top three Code of Practice guidelines.

107. 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 of time for which the product will be supported with security updates.

108. 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 implement basic security measures relating to 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.

5A(iii) - Option 2 - Mandatory Security Labelling Scheme

109. 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.

110. 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 manufacturer of the product complies with a security baseline based on the top three Code of Practice guidelines.

111. 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 proportionate due diligence to assure the retailer that the manufacturer is compliant with the security baseline.

112. As detailed in Annex 2E - Development of labelling scheme options, DSIT has undertaken extensive work to analyse the likely efficacy of both a voluntary and mandatory labelling scheme.

- DSIT undertook work with the PETRAS Consumer Security Index Project to fund and compile a rapid evidence assessment on labelling schemes for IoT security.[119,120] This included DSIT part-funding a survey study, conducted by researchers at the Dawes Centre for Future Crime at

[117] https://www.gov.uk/government/publications/the-northern-ireland-protocol
[118] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374
[119] 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
[120] Make It Clear, 2019. DCMS- IoT labelling online study.

UCL between September 2018 to January 2019, to assess the influence of different (security-related) labelling schemes on consumer choice for IoT devices.[121]

- 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.[122]

113. This option could be implemented using the powers in the PSTI Act 2022 to set out a provision requiring mandatory labels for consumer connectable products that state whether the product complies with the top 3 guidelines of the Code of Practice.

5A(iv) - Option 3 - Legislating to mandate a minimum security baseline for consumer connectable products

114. Details of the preferred policy option are captured in 5B - Description of preferred option. In summary, the intended intervention will:

- use the powers in the PSTI Act to mandate that all manufacturers of consumer connectable products making their products available in the UK comply with a minimum security baseline specified by the Secretary of State, which would initially be based on the top three Code of Practice guidelines;
- mandate that retailers, importers and distributors involved in the transmission of consumer connectable products to customers play a role in ensuring that manufacturers of these products meet the security requirements that comprise the minimum security baseline;
- ensure that manufacturers of UK consumer connectable products share information with relevant economic actors regarding their compliance with the security requirements, through self-declaring their compliance or additionally seeking third-party certification.

115. The three initial security requirements that the Government intends 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

116. DSIT has collaborated with NCSC, international partners, industry, academia, cyber security experts, and civil society in developing its preferred intervention (Option 3). The security requirements established by the Regulations mandate a minimum cyber security baseline that manufacturers of consumer connectable products made available to customers in the UK will be obligated to compliant with by 29 April 2024.

117. The initial requirements are based on the top three guidelines from the Code of Practice for Consumer IoT Security, and the equivalent provisions of ETSI European Standard (EN) 303 645: provisions 5.1-1, 5.1-2, 5.2-1, and 5.3-13.

118. The PSTI product security regime (comprising both the 2022 Act and the 2023 Regulations) places proportionate obligations on relevant economic actors involved in the manufacture and distribution of consumer connectable products, and establishes a robust enforcement regime to ensure economic actors comply with their obligations.

119. The twelve key policy positions underpinning the development of the PSTI product security regime are summarised in Box 10. 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 proposals.[123]

Box 10 - Key details of policy positions underpinning the preferred intervention (Option 3)

[121] 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/

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

[123] 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

Scope of the PSTI product security measures

Key Policy Position 1 - Detailing products in scope

The PSTI product security regime will apply to any consumer connectable products made available to customers in the UK Where the Government considers it inappropriate for certain connectable products to be captured by the regime, these products are excepted from its scope in the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023The Regulations except certain product classes.

- *The regime only applies to product lines made available to UK consumers, This includes products made available to 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 made available to businesses for use in an enterprise or industrial setting. 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 only applies in relation to consumer "internet-connectable products" and consumer "network-connectable products", as defined in Section 5 of the PSTI Act.*
- *The initial security requirements relate to the physical product, and where appropriate, software connected to the manufacturer's intended purpose for the product, whether or not that software is installable on the product.*
- *Wherever practical, the legislation will apply to all activity that could lead to vulnerable products being made available to consumers (see Section 55 of the PSTI Act for further details).*

Key Policy Position 2 - Exempted product classes

Specific product classes that would otherwise fall within the scope of this regime, but for which it would be inappropriate for it to apply, are excepted from the regime in the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023.

- *To ensure businesses are not subject to an unnecessarily duplicative regulation, product classes that are subject to comparable UK cyber regulation, either currently or in the near future, are excepted from the regime. These are:*
  - *Products to which certain EU Legislation applies, where these products are made available for supply in Northern Ireland*
  - *Charge points for electric vehicles*
  - *Medical devices*
  - *Smart Meters and certain associated products*
- *Products that the Government has deemed disproportionate to regulate at this stage are also excepted from the regime. These are:*
  - *Desktop computers*
  - *Laptop computers*
  - *Tablet computers which do not have the capability to connect to cellular networks*

Key Policy Position 3 - Adaptable scope

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

Key Policy Position 4 - Interoperability

The Government is committed to ensuring that the PSTI product security regime remains interoperable with other existing or planned government interventions covering

contiguous, or overlapping product classes

Role of economic actors

Key Policy Position 5 - Obligations on economic actors

The regime places proportionate obligations on relevant economic actors involved in the manufacture, import and distribution of in scope products to consumers to ensure that insecure consumer connectable products are not made available to customers in the UK. These obligations are set out in Chapter 2 of the Act.

Key Policy Position 6 - Security Requirements

The legislation obligates relevant economic actors to not make consumer connectable products available in the UK unless the manufacturer of the product complies with a mandatory security baseline.

- *The initial security requirements are based on 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 and easily guessable 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.*
  - *Security Requirement 2 (Implement a means to manage reports of vulnerabilities) - manufacturers will need to provide a point of contact for the reporting of security issues affecting the product, and publish information setting out how these reports will be managed.*
  - *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 PSTI Act 2022 allows Ministers to revoke, update or introduce new security requirements on manufacturers, importers and distributors of relevant connectable products.

Key Policy Position 8 - Product Assurance

Where changes to the wider technological or threat landscapes render it appropriate, the PSTI Act 2022 enables Ministers to mandate product assurance for particular categories of consumer connectable products.

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. The enforcement authority is expected to be the Office for Product Safety and Standards (OPSS).

Key Policy Position 10 - Enforcement role and responsibilities

To enable proportionate enforcement across a range of contexts, the PSTI Act 2022 provides the enforcement authority with necessary powers, as well as the ability to issue appropriate enforcement notices and penalties.

Key Policy Position 11 - Appeals

Relevant economic actors will have the right to appeal any enforcement notices or sanctions imposed on them.

Key Policy Position 12 - Proportionate transitional provisions

The Government announced its intention to mandate security requirements based on the top three Code of Practice guidelines in January 2020. A commitment was later made to provide a 12 month implementation period for affected businesses to finalise changes to their business practices. On 29 April 2023, the Government published the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 in draft, and announced the start of the regime's 12 month implementation period.

5C - How the preferred option will be given effect

120. An earlier impact assessment (RPC-DCMS-4353(2)) supported the product security measures of the PSTI Act 2022. This Act established a framework for regulating consumer connectable product cyber security by:

- **defining products in scope of the regime**;
- **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 enforcement and investigatory powers,enforcement notices, and sanctions available to the appointed enforcement authority; and
- **Establishing delegated powers** enabling theSecretary of State to set out or update key elements of the regime using secondary legislation.

121. Best endeavours were made in the earlier impact assessment to capture the full impact of the intended legislative approach. However, to ensure that the PSTI product security regime remains effective amidst changes to the threat or technology landscapes, the Government is using secondary legislation to introduce key elements of the regime. See Box 9 for further details of the intended legislative framework, and steps the Government is taking to ensure it remains effective over time.

122. The instrument that this impact assessment relates to defines:

- The initial three security requirements;
- Conditions for deemed compliance with the initial three security requirements;
- Products to be excepted from the security requirements; and
- The minimum information required to be included in a statement of compliance and the minimum length of time for which manufacturers and importers will be required to retain a copy of the statement of compliance.

123. 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.

5D - How the intervention would meet our policy objectives

124. 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 cyber security measures relating to consumer connectable products.

125. The view of NCSC - the UK's technical authority for cyber threats, is that compliance with the initial minimum security baseline that the secondary legislation 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).

126. The Government intends to reduce the risk of the harms that may arise from vulnerable consumer connectable products by introducing the following three requirements:

- **A ban on universal default and easily guessable 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 for** - 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.

127. 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

128. The Government intends for the PSTI product security regime to come into effect on 29 April 2024.

Section 6 - Proportionality approach

6A - Extent of analysis and further impact assessment publications

129. 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 medium impact measure, as a result of:

- the estimated Equivalent Annual Net Direct Cost to Business (EANDCB) being greater than +/- £10 million but less than +/- £50 million;
- the considerable number of businesses that will be affected;
- the substantial change to existing requirements the preferred option represents; and
- the multiple factors that need to be considered to estimate the impact of the measure.

130. DSIT considers this measure to be at the higher end of the medium impact category, as the Net Present Social Value (NPSV) of the preferred option exceeds the +/- £50m threshold, due to the fact that the benefits of the measure have not been monetised.

131. Therefore, as far as possible in the context of the fundamental barriers to gathering representative evidence for some key cyber crime variables, we are 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.

132. The previous impact assessment followed RPC guidance on the assessment and scoring of primary legislation measures, and sought to provide an indicative view of the likely scale of impacts of the whole PSTI product security regime, including the effects of the elements expected to be included in the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023. This impact assessment expands on this, incorporating new evidence to reflect the changes that have occurred in the cyber security landscape. At the primary legislation stage, the RPC validated an EANDCB figure of £23.9m for the PSTI Product Security regime. The Government's estimate of the direct cost to business has been refined as part of this secondary legislation impact assessment due to an updating of assumptions and removal of the benefits estimation which was based on heavily uncertain assumptions. Specifically, the changes in this impact assessment compared to the previous one are outlined below:

- The assumptions and figures relating to non-compliant devices have been updated
- The assumptions around the number of disposable devices have been updated
- The benefits model has been replaced with a break-even analysis
- Updated cost figures with relevant data have been used where possible
- The implementation date has been updated in line with policy developments
- A competition analysis has been included

133. This impact assessment seeks validation of an EANDCB for the preferred option of £21.8m. There has not been a formal consultation to specifically inform this secondary stage impact assessment, as the policy has not changed since primary stage. There was, however, a formal consultation which helped inform the primary stage assessment. The EANDCB differs at secondary stage due the removal of benefits, and an updating of assumptions which have largely been informed by bilateral engagement with stakeholders. Details of these updates are included later in the assessment.

134. An overview of the evidence base used in this cost benefit assessment can be seen in Box 11.

Box 11 - Overview of the evidence base underpinning the cost benefit assessment detailed in this impact assessment

This impact assessment builds on previous work 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 3D - Previous UK Government Interventions, DSIT 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, including tasking external suppliers with conducting two business surveys and three consumer surveys.

DSIT 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 intends to mandate. This work has also been supported by extensive additional engagement by NCSC and DSIT with industry to gather information and test assumptions.

135. The secondary legislation instrument that this impact assessment applies to utilises powers provided in the PSTI Act. DSIT has therefore sought to provide a robust analysis of the likely impacts of our policy measure as a whole. It covers the cost-benefit analysis of bringing into force the product security regime overall, including the impact of provisions in both Part 1 of the PSTI Act and this instrument. Box 12 contains an overview of key policy considerations during the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 development process.

Box 12 - Overview of secondary legislation development policy considerations

Adaptable scope

As detailed in 5B - Description of preferred option, the product security measures in the PSTI Act allow the Secretary of State to update the scope of products this legislation will apply to. The legislation enables 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.

This secondary legislation excepts five product classes from the scope of the regime:

- Certain products when made available to be supplied in Northern Ireland
- EV charge points
- Medical devices
- Smart Meters
- Conventional IT

Identity of the enforcement authority

The Government has announced that it intends to appoint the Office for Product Safety and Standards (OPSS) to enforce the PSTI product security regime. OPSS is the national enforcement authority for all consumer products. They enforce a wide range of product regulation covering products that also fall in scope of this regime, and so are well placed to regulate it once it comes into force. This impact assessment takes into consideration the funding required by OPSS to provide enforcement, as well as their current skills, knowledge and staffing levels as an enforcement authority.

Minimum requirements for the statement of compliance

The secondary legislation sets out specific requirements for manufacturers and importers in relation to the statement of compliance. This defines the level of input required from these businesses and is reflected in this analysis.

136. The policy considerations outlined above have not affected the EANDCB since the primary stage Impact Assessment. The Government's intention for the connectable product classes to be regulated by this regime when it first comes into effect is unchanged since the previous Impact Assessment. Furthermore,

the Government has confirmed the identity of its intended enforcement authority for the regime - the Office for Product Safety and Standards. This also does not affect the EANDCB as costs to the enforcement authority were estimated in the previous Impact Assessment and these estimates continue to remain the same. Also, these costs to the enforcement authority do not impact business and so therefore do not affect the EANDCB. The previous IA included a conservative estimate of the cost to businesses for drawing up and verifying a statement of compliance. This estimate is reflected in the analysis below as the level of input required from businesses was accounted for in the previous IA and does not translate to higher costs that would impact the EANDCB.

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

137. 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.

138. Using the gathered evidence, DSIT 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.

139. DSIT's approach to modelling the benefits of this intervention arises from an assumption that implementation of the regime's security requirements 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).

140. Whilst DSIT 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 DSIT 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.

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), [DSIT's] estimates highlighted above are reasonable".

141. In addition to this, a potential unintended consequence of policy option 2 and 3 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 7D(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 [DSIT'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."

142. Overall, DSIT has gone to great lengths to fill evidence gaps but due to the inherent challenges involved in identifying cyber crime; low response rates in DSIT commissioned surveys; or due to challenges associated with forecasting how businesses will respond to the proposals, some evidence gaps remain. In these instances, DSIT has used assumptions alongside the best available evidence in order to quantify the impact of the proposed policy options. A detailed list of risks and assumptions can be seen in Annex 3 - Risks and Assumptions.

Section 7 - Cost-Benefit Analysis

143. **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 the modelling of any benefits and costs** that would result from the shortlisted policy interventions.

144. In the previous Impact Assessment, the benefits of this policy were quantified. On reflection, building upon the work already conducted and based on advice from the RPC, DSIT has decided, for this impact assessment, to undertake a break-even analysis. This reflects the challenge that despite our best endeavours, the benefits of this policy are extremely hard to calculate as highlighted in NCSC Statement 4.

145. Table 1 summarises the outputs of the Cost-Benefit model for the three shortlisted policy interventions (detailed in 5 - Shortlisted policy interventions). It should be noted that the shortlisted policy interventions have been assessed against the 'do nothing' option (Option 0). Similar to the primary legislation 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 Cost-Benefit Analysis: 10 Year Net Present Value (£m)

Shortlisted policy option	Low Scenario	Central Scenario	High Scenario
Option 1 (Do-minimum) Voluntary security labelling scheme	-£10.4m	-£21.3m	-£25.9m
Option 2 (Other viable option) Mandatory security labelling scheme	-£60.7m	-£129.5m	-£156.1m
Option 3 (Preferred option) Mandate a cyber security baseline based on the top three Code of Practice guidelines	-£90.0m	-£193.2m	-£222.0m

146. 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% per annum 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 2019, while the Present Value (PV) base year is 2020.

147. 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). However challenges have included:

- Low response rates to surveys. Two surveys sent to over 2,000 companies only received replies from 22 consumer IoT manufacturers and 12 retailers.
- There is limited data available on the number of staff who work at different IoT manufacturers.
- The costs of a cyber attack on consumers has been poorly studied, and is hard to estimate given the range of different attacks and possible outcomes.
- There is limited information on the environmental costs of disposal of different types of IoT devices.

148. Despite the limitations of some of the data used, the figures presented in this impact assessment are based on the best available data.

149. 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 costs of each modelled policy intervention.

Table 2 - Overview of modelled costs per shortlisted policy option (central estimate, PV 2020)

Modelled costs	**Option 1** *Voluntary label*	**Option 2** *Mandatory label*	**Option 3** *Mandatory baseline*
Impacts on **manufacturers**			
Cost: Familiarisation with the regulation	**£0.2m**	**£0.2m**	**£0.4m**
Cost: Self-assessment against the security baseline	**£0.2m**	**£9.3m**	**£9.3m**
Cost: Labelling		**£5.3m**	
Cost: Implementing security improvements			**£26.3m**
Cost: Publication of a statement of compliance			**£2.0m**
Impacts on **retailers**			
Cost: Familiarisation with the regulation	**£5.0m**	**£5.0m**	**£14.2m**
Cost: Disposal of non-compliant goods		**£88.0m**	**£88.0m**
Cost: Verification of a statement of compliance			**£1.7m**
Impacts on **Enforcement Authority**			
Cost: Enforcement		**£5.9m**	**£5.9m**

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

	Option 1 *Voluntary label*	**Option 2** *Mandatory label*	**Option 3** *Mandatory baseline*
Costs			
Familiarisation cost	Direct Impact	Direct Impact	Direct Impact
Self-assessment cost	Direct Impact	Direct Impact	Direct Impact
Labelling cost	Direct Impact	Direct Impact	
Costs of disposing non-compliant goods		Direct Impact	Direct Impact
Costs associated with Statement of Compliance			Direct Impact
Costs associated with Verification of compliance			Direct Impact
Costs associated with providing Security Improvements		Indirect Impact	Direct Impact
Regulator costs	Does not directly impact businesses	Does not directly impact businesses	Does not directly impact businesses

7A - Structure of the Cost-Benefit Analysis

150. For ease, this 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 cost of cyber attacks*
- **Section 7C - Costs methodology of relevance to all options:** This section details the approach taken to estimating the costs that would arise, to varying extents, from implementing the aforementioned shortlisted options:
  - *7C(i) - Estimating the number of manufacturers and retailers of consumer connectable products*
  - *7C(ii) - Estimating familiarisation costs*
  - *7C(iii) - Estimating self-assessment costs*
  - *7C(iv) - Estimating costs to retailers*
- **Section 7D - 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:
  - *7D(i) - Estimating the costs of labelling*

- *7D(ii) - Estimating the costs of implementing security improvements*
- *7D(iii) - Estimating the costs of publishing and verifying a statement of compliance*
- *7D(iv) - Estimating the costs associated with the disposal of non-compliant goods*
- *7D(v) - Estimating the costs of enforcement*

151. 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** - Analysis of the impact on medium sized businesses*
- ***8D** - Break-Even Analysis*
- ***8E** - Analysis of potential trade impacts*
- ***8F** - Equalities Impact Assessment*
- ***8G** - Assessment of impact on innovation*

7B - Underlying methodology common to all options

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

Estimating growth in the number of consumer connectable products

152. Adoption of IoT products in the UK is predicted to grow into the future, with some estimates predicting 156 million devices by 2024.[124] Forecasts suggest that there could be up to 29.4 billion connectable devices worldwide by 2030.[125] 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.

153. 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 connectable products (with the exception of conventional IT products such as smartphones and tablets with a cellular connection) from 2017 to 2024.[126] The five criteria used to define IoT in the Ofcom research[127] are that devices must:

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

154. This research does not include connectable products that are typically regarded as "conventional IT" such as smartphones, however smartphones 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 2025'[128] in order to estimate the total number of consumer connectable products within scope over time.

155. Similar to the research from Ofcom, the forecast does not cover the entire appraisal period for this policy intervention, which goes until 2032. 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%, low scenario estimate 5.5%, high scenario 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%.[129]

---

[124] Cambridge Consultants, 2017. Connected Nations Report 2017: Data Analysis.

[125] Strategy Analytics, 2019. Accessed from: Statista, 2022. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/ [accessed: 26 October 2022].

[126] Ofcom, 2017. Connected Nations Report 2017: Data Analysis.

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

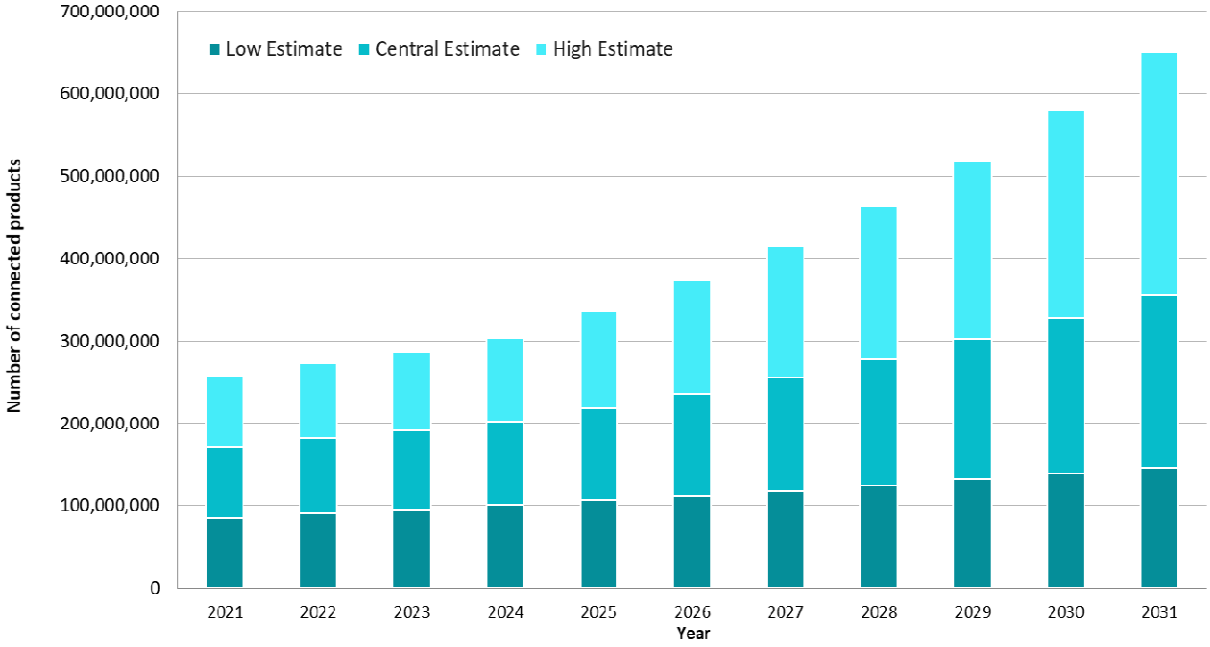
[128] https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/

[129] https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030

Sensitivity analysis around the best estimate has been included. The growth rate of the central estimate has been halved to produce the low case scenario and increased by 50% to achieve the high scenario estimate.

156. 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 connection rate of consumer connectable products

157. 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.

158. According to the RSM survey commissioned by DSIT, consumers reported that on average, 4% of devices were used, but not connected to the internet, while 3% were owned but not used.[130] 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.

Estimating the proportion of overall products from each product group

159. Respondents to a representative consumer survey conducted on behalf of DSIT, reported ownership of consumer connectable products within three high level product groups as follows:[131]

- **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

160. These estimates are similar to recent findings from Ofcom, with Ofcom's 2022[132] findings suggesting that the ownership levels above may in fact be a slight underestimate. Although Ofcom's research uses different breakdowns of product groups so the findings cannot be compared directly, DSIT is assured that the values are representative of the increasing level of ownership of IoT devices.

[130] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
[131] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
[132] Ofcom, 2022. Tech Tracker 2022 Subset data tables.

161. The consumer connectable products types included in the product groupings used in the RSM survey (outlined in Box 13) 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 (1.59[133]) compared to connecting the home products (2.94[134]). 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 7D(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.

Box 13 - 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*

162. 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 category[135] (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 - DSIT assumes 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%

7B(ii) - Estimating the cost of cyber attacks against IoT devices

163. 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);
- **Average unit cost** of an attack.

Estimating the frequency of a successful attack occurring

164. 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 5) from the Crime Survey for England and Wales and (ii) data on the number of consumer connectable products in the UK.[136]

[133] 1.59 devices owned by households (based on a sample of consumers that reported owning at least 1 device).

[134] 2.94 devices owned by households (based on a sample of consumers that reported owning at least 1 device)

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

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

Table 5 - Data on fraud and computer misuse incidents in England and Wales classified as cyber crime

	Fraud			Computer misuse incidents			Overall
	Total incidents	% Cyber Crime	Total cyber incidents	Total incidents	% Cyber Crime	Total cyber incidents	Total cyber incidents
Mar 2019	3,809,000	54%	2,056,860	966,000	97%[137]	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

165. 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%[138] (8.8% in the high scenario estimate and 4.4% in the low case scenario).

- The risk with this assumption is that it assumes each attack occurs on a different device. This means that the number of compromised devices ends up being lower and therefore the breakeven analysis done later in the document becomes an underestimate. There is a significant likelihood that some unsecured devices will be breached several times, not just the once that the 4.4% depends on. This makes it more likely to be achieved.

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

"NCSC agrees with DSIT'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".*

Average unit cost of an attack

166. To conduct a break-even analysis, 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).[139] However, this estimate includes the 'anticipation of crime'

[137] Note that the proportion of computer misuse incidents identified as cyber crime was not available for the year ending March 2019, therefore DSIT assumes that this will remain constant at 97%.
[138] 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.
[139] Heeks M., Reed S., Tafsiri M., Prince S., 2018. The economic and social costs of crime Second edition

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 economic and social costs of crime.[140] Furthermore, data from the Cyber Security Breaches Survey of 2022 has been used to estimate the unit cost of an attack to businesses, and this has been expressed in 2019 prices.

167. 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

168. 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.

169. 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'[141] 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, DSIT has taken a conservative approach to estimating the unit cost of a cyber attack. Note: this cost does not cover all the costs associated with cyber crime, there is no data for costs such as police and victim service costs.

170. 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 6.

Table 6 - 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		***B***		***C***		***D***		***E***		***ABCDE***
Consumers	1.35bn	x	82%	x	4.4	x	55%	x	£282	=	£14.8bn
Businesses		x	18%	x		x	46%	x	£1,081	=	£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)*

171. This calculation helps to frame the scale of the issue that the PSTI product security regime aims to act against.

[140] Heeks M., Reed S., Tafsiri M., Prince S., 2018. The economic and social costs of crime Second edition
[141] Heeks M., Reed S., Tafsiri M., Prince S., 2018. The economic and social costs of crime Second edition

7C - Costs methodology of relevance to all options

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

172. 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.

173. The IoTUK Nation Database provides a list of UK IoT businesses which could be in scope of the PSTI product security regime.[142] This database, last updated in August 2018, includes 69 IoT manufacturers of computer, electronic and light electrical products, which has been used as the low 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.[143]

174. DSIT has assumed that the number of IoT manufacturers will grow over the appraisal period by 3% per annum. The 3% is consistent with the growth of businesses in the UK economy over the period 2000-2020, as taken from the BEIS Business Population Estimates[144]. Table 7 below shows the total number of manufacturers in each year of the appraisal. For simplicity of showing the results, the businesses in year 1 will be shown in the tables below.

Table 7 - Estimated number of manufacturers through the appraisal period

	Low Scenario	Central Scenario	High Scenario
2023	69	170	170
2024	71.1	175.1	175.1
2025	73.2	180.4	180.4
2026	75.4	185.8	185.8
2027	77.7	191.3	191.3
2028	80.0	197.1	197.1
2029	82.4	203.0	203.0
2030	84.9	209.1	209.1
2031	87.4	215.4	215.4
2032	90.0	221.8	221.8

175. 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

[142] https://datamillnorth.org/dataset/iotuk-nation-database
[143] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
[144] https://www.gov.uk/government/statistics/business-population-estimates-2020/business-population-estimates-for-the-uk-and-regions-2020-statistical-release-html#:~:text=Between%202000%20and%202020%3A,and%20between%202013%20and%202014

approach has been taken which assumes that all costs incurred as a result of regulatory options on manufacturers fall on UK business activity.

176. 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 3,485 retailers in 2020.[145] This estimate has been used for both the central and low estimate. However, in the high scenario DSIT estimates that there are 3,675 retailers within scope.[146] It is important to note that the estimated number of retailers in scope is likely to be an underestimate as there may be retailers who sell consumer connectable products but do not fall in the 'retailers within the electrical appliances' category. 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 the legislation as, if they sell or otherwise supply new consumer connectable products, they will fall under the PSTI Act distributor definition and will need to comply with duties in the Act. In both the worst case and central scenario, DSIT estimates that there are 11,200 charities within scope. These estimates are based on data from the Charity retail association.[147] The central estimate has been reduced by 50% to estimate the low case scenario.

7C(ii) - Estimating familiarisation costs

177. Under all scenarios, both manufacturers and retailers will have to spend time familiarising themselves with the legislation. RSM conducted a survey on behalf of DSIT to collect evidence on the time it would take for organisations to familiarise with different regulatory options, and the job roles that would be involved.[148] 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 8 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 7C(i) - Estimating the number of manufacturers and retailers of consumer connectable products).

Table 8 - Salary Assumptions

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.

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

[145] https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/

[146] 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/

[147] 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.

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

Other	£124	£32,284	Average national wage (ONS)

Policy Options 1 and 2 - ***Labelling Scheme Options***

178. Both manufacturers and retailers would have to spend time familiarising with the regulation and the implications for their businesses. Even in Option 1, manufacturers would need to familiarise themselves with the regulation to decide if they wish to opt in, since opting out would indicate to the consumer that their product does not meet the scheme's minimum security baseline. 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 £1,585. However, to account for the small sample size (only four manufacturers responded) sensitivity analysis has been used (the low estimate has been reduced by 20% in the high case scenario and increased by 20%).

179. 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.

180. Retailers, like manufacturers, were asked to estimate the one-off familiarisation costs, in terms of staff time, to read and understand proposed regulation 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 days.[149] 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.

Table 9 - Estimated cost of familiarisation with security labelling per organisation Policy Option (1+2)

	Low Scenario	**Central Scenario**	**High Scenario**
Average cost per Manufacturer	£1,268	£1,585	£1,902
Number of Manufacturers (year 1)	69	170	170
Total cost to Manufacturers (2019 prices, in PV terms)	£74,332	£228,922	£274,706
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, in PV terms)	**£10,350,525**	**£20,910,126**	**£25,414,276**
Overall cost (2019 prices, £m) in PV terms	**£10.4m**	**£21.1m**	**£25.7m**

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

*Policy Option 3 - **Mandatory security baseline***

181. 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 overheads like non-salary costs such as National insurance contributions.

Table 10 - Estimated average cost of familiarisation with the initial three security requirements per organisation Policy Option (3)

	Low Scenario	Central Scenario	High Scenario
Average cost per Manufacturer	£1,972	£2,465	£2,958
Number of Manufacturers (year 1)	69	170	170
Total cost to Manufacturers (2019 prices)	**£115,602**	**£356,020**	**£431,124**
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)	**£29,523,311**	**£59,648,755**	**£72,502,088**
Overall cost (2019 prices, £m) in PV terms	**£29.6m**	**£60m**	**£72.9m**

7C(iii) - Estimating self-assessment costs

182. 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 in relation to which they are compliant and which they are not) as part of their self-declaration. This declaration is mandatory under both Policy Option 2 - Mandatory security labelling scheme and Policy Option 3 - Mandatory security baseline.

183. Throughout the appraisal period all manufacturers will face a recurring self-assessment cost. For the purpose of this analysis, DSIT assumes 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, as well as the type of job roles that would be involved. This information was multiplied by the wages highlighted in Table 8 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.

184. 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 high case scenario and £5,260 in the low 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 overheads like non-salary costs such as National insurance contributions.

Table 11 - Self-assessment costs for mandatory policy options through the appraisal period (2&3)

	Low Scenario	Central Scenario	High Scenario
Average cost (2020 prices)	£5,260	£6,575	£7,890
Number of Manufacturers (year 1)	69	170	170
Total Real cost (2019 prices, £m) in PV terms	**£3.0m**	**£9.3m**	**£11.2m**

185. In contrast to the mandatory options (Policy options 2+3), self-assessment is not mandatory for **Policy Option 1 - voluntary security labelling scheme.** DSIT assumes that only those manufacturers who already comply with the security requirements will opt to undertake a self-assessment as they will stand to gain from adopting the security label due to competitive pressure (i.e. those who meet the minimum security bar would appear not to meet the security conditions to consumers if they do not opt in). 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 practice. 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. DSIT assumes that 1.8% of manufacturers adopt the label in the high case and 0.39% in the low case as exhibited below.[150] DSIT has included these as part of direct costs as this will likely drive a direct behavioural change, even though the government would not require it.

Table 12 - Estimated self-assessment costs for manufacturers throughout the appraisal period (1)

	Low Scenario	Central Scenario	High Scenario
Average annual cost per manufacturer (2020 prices)	£5,260	£6,575	£7,890
Number of manufacturers adopting voluntary label	0.39%	1.8%	1.8%
Number of Manufacturers	69	170	170
Total Real cost (2019 prices) in PV terms	**£11,779**	**£167,265**	**£176,561**

7C(iv) - Estimating costs to retailers

*Policy Option 1 and 2 - **Labelling scheme options***

186. 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:

[150] See footnote 107 for more detail on the rationale for this assumption.

- 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 7D(iv) - Estimating the costs associated with the disposal of non-compliant goods.

*Policy Option 3 - **Mandatory security baseline***

187. 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 7D(iii) - Estimating the cost of publishing and verifying a statement of compliance).

Table 13 - Total direct cost to retailers under the preferred (3) and other shortlisted policy options (1&2) (2019 prices, 2020 PV)

	Low Scenario	Central Scenario	High Scenario
Policy Option 1 - **Voluntary Security Label**	£4m	£5m	£6.3m
Policy Option 2 - **Mandatory Security Label**	£4m	£5m	£6.3m
Policy Option 3 - **Mandatory Security Baseline**[151]	£12.3m	£15.9m	£21.7m

7D - Cost methodology not of relevance to all options

7D(i) - Estimating the costs of labelling

188. Under the voluntary labelling scheme option (Option 1) DSIT assumes that the introduction of the scheme will not:
    - place additional labelling costs onto manufacturers; or
    - increase costs for consumers.

189. These assumptions have been made for the following reasons:
    - Firstly, DSIT assumes 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, DSIT assumes 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.[152] Therefore, in this scenario DSIT assumes that costs will be incorporated as part of manufacturers regular update cycle and not passed onto consumers.

*Policy Option 2 - **Mandatory security labelling scheme***

190. The cost of labelling will be incurred by all manufacturers of consumer connectable products selling their products on the UK market under Policy Option 2. 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

[151] 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.

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

packaging redesign cycle.[153] Therefore, DSIT assumes that this will impose an additional cost on all manufacturers in scope.

191. 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 of the mandatory label. However, research on the cost of labelling changes for food manufacturers states that it is unlikely that manufacturers would opt for a stick on label for the following reasons:[154]

- 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.

192. In line with the evidence cited above, DSIT assumes 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, DSIT 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 14.

Table 14 - Evidence on the cost of product labelling

Research Subject	Source	Estimated cost of 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

193. At the end of 2019, research was also commissioned 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).[155]

194. 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.[156] 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 15). The total impact was estimated by multiplying the average cost per manufacturer by the estimated number of manufacturers in the UK. The low 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.[157] 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.[158]

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

[154] 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

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

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

[157] https://datamillnorth.org/dataset/iotuk-nation-database

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

195. For the purpose of this impact assessment, DSIT assumes 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 13, 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 15). This figure accommodates relatively higher estimates provided by a few large firms while also allowing for lower cost estimates faced by small/micro businesses. 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.

196. 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 eight, whilst the mean is 21 products.[159]

197. 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.[160]

Table 15 - Estimated labelling costs (Policy Option 2)

	Low Scenario	Central Scenario	High Scenario
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 (year 1)	69	170	170
Total cost to UK consumer connectable product manufacturers (2019 prices, PV 2020)	**£2.1m**	**£5.3m**	**£13.8m**

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

198. DSIT assumes that although the cost of implementing security improvements primarily pertains to Policy Option 3, businesses may incur an indirect cost associated with making security improvements in Policy Option 2 as well. This is because a mandatory labelling scheme would incentivise businesses to make security improvements as their level of compliance would be transparent to consumers, and some consumers in the market would prefer to purchase more secure consumer connectable products. At this stage it is not possible to quantify this indirect cost as there is not enough evidence to buttress assumptions surrounding consumer purchasing behaviour or manufacturers sensitivity to competitive pressures.

199. DSIT has engaged with industry to attempt to gather evidence on the cost impact of the three security requirements under Policy Option 3 - 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

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

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

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 universal default passwords but more detail was given on the cost impact associated with implementing a vulnerability disclosure policy and security updates.

200. 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 8, in order to estimate the financial cost of this time.[161] 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).

Universal Default passwords

201. The market study and accompanying review of literature undertaken by RSM found very few products explicitly supplied with universal 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 universal 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.

202. 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, DSIT estimates that this requirement will impose additional costs for 10% of manufacturers.

203. The RSM market survey did not return information on the cost impact associated with removing universal default passwords. DSIT attempted to gather further information on the costs that security requirements based on 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.

204. Without more robust data, the exact cost of eliminating universal default passwords is unclear. Therefore, the cost of implementing this security requirement has been estimated by taking the mean of the average reported cost of implementing a vulnerability disclosure policy (second security requirement) and publishing the minimum length of support for security updates (third security requirement) as the closest proxy. Hence, the estimated average annual cost used for this analysis is £10,918 and DSIT assumes that this remains constant throughout the appraisal period. As this calculation is based on the above assumptions, sensitivity analysis has been applied to this estimate. The central estimate has been increased by 20% in the high case scenario and decreased by 20% in the low scenario.

205. Table 16 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.

Vulnerability disclosure policies

206. 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 policy. This is likely an overestimate. Research conducted by IoTSF revealed that only 27.1% of companies have a vulnerability disclosure policy. This has

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

been taken as the best estimate available. To this end, DSIT estimates that around 73% of manufacturers will incur additional costs associated with implementing this security requirement[162].

207. Although the results also show that the overall impact of mandating a requirement based on this Code guideline would be low or zero in many cases, even companies with a policy would bear some familiarisation costs to ensure that it was fully compliant with the 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 £4,559 per manufacturer in 2019 prices.

Security updates

208. According to the RSM survey, unlike the vulnerability disclosure policy requirement, few manufacturers published a minimum length of time for which security updates will be provided. Out of 17 respondents only four provided this information to consumers for all their products. Mandating this (as in the preferred intervention - Policy Option 3) 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 DSIT estimates 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 two. Year one costs are higher because they account for additional costs associated with the implementation of this security requirement. It is important to note that this is likely to be an overestimate, as some manufacturers in the RSM survey suggested that this cost would likely be low "as it would only involve updating online/user guidance content".[163]

Table 16 - Costs associated with Implementation of the Security Requirements in PV terms (Policy Option 3)

	Optimistic case	Central Estimate	Worst case
Security Requirement 1 - **Ban universal and easily guessable default passwords**			
% of Manufacturers that have to make changes	10%	10%	10%
Estimated number of manufacturers affected (year 1)	7	17	17
Average annual cost per manufacturer (2019 prices)	£8,347	£10,918	£13,102
Total Cost over appraisal period (£m):	**£0.5m**	**£1.6m**	**£2.0m**
Security Requirement 2 - **Publish information on how to report security issues**			
% of Manufacturers that have to make changes	73%	73%	73%
Estimated number of manufacturers affected (year 1)	50	124	124

[162] Copper Horse. The state of Vulnerability Disclosure policy (VDP) usage in Global Consumer IoT in 2022

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

Average annual cost per manufacturer (2019 prices)	£4,559	£4,559	£4,559
Total Cost over appraisal period (£m):	**£2.0m**	**£5.0m**	**£5.0m**
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 (year 1)	**68**	**167**	**167**
Average annual cost per manufacturer (2019 prices)	**£17,277 in year one £12,958 from year two**	**£17,277 in year one £12,958 from year two**	**£17,277 in year one £12,958 from year two**
Total Cost over appraisal period (£m):	**£8.0m**	**£19.7m**	**£19.7m**
Overall Cost (all three security requirements, 2019 prices, £m):	**£10.5m**	**£26.3m**	**£26.7m**

209. Overall, the estimated additional cost of implementing security improvements to meet the minimum security baseline in Policy Option 3 is £26.3m in the central estimate, £26.7m in the high case and £10.5m in the low 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 and easily guessable 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.

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

Statement of Compliance cost

210. Under the preferred option (policy option 3), manufacturers are required to draw up a statement of compliance that accompanies an in-scope product when making it available. The estimated staff cost of providing security update information has been used as a proxy for the staff cost of providing a statement of compliance. 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. 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 central and high estimate while 69 in the low estimate), which brings the total cost (across all manufacturers) to £2m[164]. The methodology for estimating this cost is summarised in Table 17.

Table 17 - Manufacturer Statement of Compliance costs (Policy Option 3)

	Low case	Central Estimate	High case
Estimated cost per manufacturer	£12,958	£12,958	£12,958
Estimated number of manufacturers (year 1)	69	170	170

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

Total cost to UK consumer connectable product manufacturers (2019 prices, PV 2020)	**£0.8m**	**£2m**	**£2m**

Verification of the Statement of Compliance

211. Distributors of consumer connectable products, under policy option 3, will be required to verify that a product is accompanied by a statement of compliance. In order to estimate the cost of this obligation the following assumptions have been made:

- Firstly, DSIT assumes 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 used[165]. The salary assumptions used account for non-salary costs such as national insurance costs. This was done to combine the data in the Annual Survey of Hours and Earnings and the Labour Force Survey.
- 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 low and high case scenarios. In the low scenario, DSIT assumes 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.

212. 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 £1.7m. These salary assumptions reflect employment costs (i.e account for overhead costs). The methodology for this estimate is summarised in Table 18.

Table 18 - Verification Costs for Distributor (Policy Option 3)

	Low Scenario	**Central Scenario**	**High Scenario**
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)	£323	£581	£1,204
Number of Distributors	3,485	3,485	3,675
Total Cost (adjusted to 2019 prices, PV 2020)	**£1m**	**£1.7m**	**£3.8m**

7D(iv) - Estimating the Direct costs associated with the disposal of non-compliant goods

*Policy Option 2 - **Mandatory security labelling scheme***

213. Under this policy option, retailers in the UK would no longer be able to sell products without a security label which indicates whether the manufacturers of 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.

[165] See Table 6 for salary assumptions.

214. Broadly, businesses (retailers and manufacturers) would face two significant costs that directly result from the disposal of non-compliant goods:

- a **loss of revenue**[166] due to a higher proportion of consumer connectable products having to be disposed of; and
- the **direct cost of disposal**.

215. 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 DSIT assumes that retailers will dispose of all current stock with a universal or easily guessable 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 universal and easily guessable 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/altered even after devices have been sent to distributors. In the earlier rendition of this Impact Assessment, it was assumed that a device would be disposed of if it did not comply with Security Requirement 2 and 3. However, 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) as these are not device-based requirements. The resulting cost estimate because of this change in assumption are much lower than the previous IA. Industry was engaged to test this assumption and it has been confirmed that a device-based assumption to estimate the cost of disposal is a reasonable approach. In reality, the central estimate of 10% is still likely an overestimate for several reasons:

- Firstly, rather than disposing of stock with a label stating the product does not comply with the first three requirements it is more likely that businesses will sell connectable products (without a security label) at a reduced price.
- Secondly, the implementation 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.

216. 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 turnover[167]. 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 7B(i) - 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 of the sensitivity analysis.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.

217. Table 19 summarises the methodology used to estimate the overall value of revenue lost. The overall loss of revenue amounts to £89m (2019 prices) in the central estimate (£93.9m in the worst case and £44.5m in the optimistic scenario). Typically, direct business impact would be measured by changes to profit. In this case, lost revenue is equivalent to lost profit since by the time of disposal, the cost of goods/cost of sales

[166] Normally, direct business impact would be measured by changes to profit in Impact Assessments. In this case, lost revenue is equivalent to lost profit since by the time of disposal, the cost of goods/cost of sales has already been incurred.

[167] 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.

has already been incurred. Notwithstanding, this is likely to be a slight overestimate as there will be some 'costs of sales' not already incurred by businesses, however there is no evidence of this presently. 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.

218. 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 unit.[168] 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.

The environmental impact of disposing non-compliant goods

219. DSIT commissioned RSM International to estimate the environmental cost of disposal. However, while the direct cost to businesses from disposal has been estimated (see section 7D(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."[169] 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."[170] 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%).[171]

220. In summary, under both policy option 2 and 3 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.

Policy Option 3 - ***Mandatory security baseline***

221. In estimating the potential loss of revenue that businesses may incur due to non-compliant devices having to be disposed of[172], the same approach has been taken as to the one described for the mandatory labelling scheme above.

Table 19 - Estimating the loss of revenue resulting from the disposal of non-compliant goods **(Policy Options 2 + 3)**

	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**

[168] 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, DSIT has not added an overhead uplift to this estimate.

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

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

[171] Greenpeace. Guide to Greener Electronics, 2017.

[172] 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).

Average price of consumer connectable products[173]	**£296**	**£296**	**£296**
Estimated value of retail stock	**£255,448**	**£255,448**	**£255,448**
Estimated number of retailers	**3,485**	**3,485**	**3,675**
Total value of stock	**£890m**	**£890m**	**£939m**
% of stock disposed of as a result of intervention	**5%**	**10%**	**10%**
Loss of revenue (nearest £m):	**£45m**	**£89m**	**£94m**
Number of devices disposed of	**150,378**	**300,756**	**317,153**
Cost of disposal per device	**£9.42**	**£28.26**	**£47.10**
Total disposal cost (£m)	**£1.4m**	**£8.5m**	**£14.9m**
Overall cost of non-compliant devices (2019 prices, PV 2020, £m)	**£41.4m**	**£88m**	**£98.1m**

7D(v) - Estimating the costs to the authority of enforcing the regime

222. Under both policy option 2 and policy option 3, 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 20 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**

Table 20 - Annual Staff Cost Assumptions

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

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

223. 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 21.[174]

Table 21 - 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**

224. 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 22 breaks down the number of products sent for external testing across product categories and across three scenarios:

Table 22 - Testing cost inputs

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

225. Table 23 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 purely 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 23 - Ongoing enforcement costs

High 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

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

Staffing cost	2.5	4.0	4.0	3.0	0.2	£711,951
Overheads	-	-	-	-	-	£156,629
Testing costs	-	-	-	-	-	£59,280
Total costs	**-**	**-**	**-**	**-**	**-**	**£927,860**
Total costs (in PV terms)						**£836,877**
Aggregate costs over appraisal period (£m)						**£7.2m**

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
Total costs (adjusted to 2019 prices)	**-**	**-**	**-**	**-**	**-**	**£736,774**
Total costs (in PV terms)						**£664,528**
Aggregate costs over appraisal period (£m)						**£5.7m**

Low 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
Total costs (adjusted to 2019 prices)	**-**	**-**	**-**	**-**	**-**	**£453,453**
Total costs (in PV terms)						**£408,989**
Aggregate costs over appraisal period (£m)						**£3.5m**

Section 8- Additional Analysis

8A - Analysis of the potential costs to consumers

8A(i) - Policy Option 2 - Mandatory security labelling scheme

226. 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.[175] 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.

227. 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 firms.[176] As a result, DSIT assumes that all small and micro manufacturers and small/micro retailers will pass direct costs onto consumers through higher prices. Business Population Estimates have been used to determine the proportion of UK consumer connectable product manufacturers that are defined as 'small' and 'micro' and from this the extent to which costs will be passed onto consumers is determined.[177] DSIT assumes, 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 one and thereafter be incorporated into business as usual costs. For instance, these changes may be incorporated into usual packaging updates.

228. It is estimated that 'micro' manufacturers account for approximately 55% of IoT UK manufacturers and 'small' manufacturers account for approximately 28% of UK manufacturers producing consumer connectable products. Furthermore, using Business Population Estimates, it is also assumed that 87% of retailers are micro businesses and 12% are small businesses. 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.
- The direct cost to manufacturers is expected to be higher in year one, as manufacturers familiarise with the scheme but then drop off once manufacturers become familiar with the legislation.
- Direct costs to retailers include (i) familiarisation costs only.
- 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 24 presents the overall cost to consumers with and without the disposal of non-compliant goods included.

229. The overall cost to consumers has been calculated by multiplying the number of 'micro/small' manufacturers and 'micro/small' retailers within scope by the average direct cost per manufacturer/retailer. Using this approach, the total cost to consumers under this policy option is £15.5m in the central scenario (£8.2m in the low scenario and £16.8m in the high scenario). It is worth noting that this is a transfer from businesses to consumers rather than an extra cost.

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

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

[177] 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 24 - Total indirect cost to consumers across the appraisal period (Policy Option 2 - Mandatory security label)

Grade	Low Scenario	Central Scenario	High Scenario
Total average direct cost to manufacturers	£40,477 in year 1 falling to £4,955 thereafter	£42,014 in year 1 falling to £6,193 thereafter	£99,335 in year 1 falling to £7,432 thereafter
Estimated number of 'micro' manufacturers (year 1)	38	94	94
Aggregate direct cost to 'micro' manufacturers (in PV terms, £m)	£2.9m	£7.1m	£7.1m
Estimated number of 'small' manufacturers (year 1)	19	47	47
Aggregate direct cost to 'small' manufacturers (in PV terms, £m)	£1.4m	£3.5m	£3.5m
Aggregate direct cost to small and micro manufacturers (in PV terms, £m)	**£4.3m**	**£10.6m**	**£10.6m**
Total direct cost to retailers	£1,263	£1,579	£1,894.27
Estimated number of 'micro' retailers	3015	3015	3179
Aggregate direct cost to 'micro' retailers (in PV terms, £m)	£3.4m	£4.3m	£5.4m
Estimated number of 'small' retailers	429	429	452
Aggregate direct cost to 'small' retailers (in PV terms, £m)	£0.5m	£0.6m	£0.8m
Aggregate direct cost to retailers	**£3.9m**	**£4.9m**	**£6.2m**
Overall cost to consumers	**£8.2m**	**£15.5m**	**£16.8m**

8A(ii) - Policy Option 3 - Mandatory security baseline

230. The same methodology and assumptions have been used to estimate the potential cost to consumers across both Policy Option 2 (Mandatory Security Label) and Policy Option 3 (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 comprise:

- familiarisation costs;
- self-assessment costs;
- costs relating to the statement of compliance; and
- costs associated with implementing changes related to the security requirements.

231. From year two direct costs to manufacturers comprise (i) self-assessment costs and (ii) costs associated with implementing changes related to the security requirements, therefore, the costs have been calculated throughout the appraisal period. 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. Similarly to policy option 2, costs associated with the disposal of non-compliant goods are also included in the analysis. The overall cost to consumers with and without the costs associated with the disposal of non-compliant goods can be found within Table 25.

232. Assuming that 55% of manufacturers are micro, 28% are 'small' and 87% of retailers are 'micro', 12% businesses are 'small', the overall direct cost to consumers is £61.0m in the central scenario (£28.6m in the low case scenario and £71.1m in the high case scenario). As mentioned above, in estimating the costs to consumers, only the direct costs to manufacturers have been accounted for.

Table 25 - Indirect cost to consumers across the appraisal period (Policy Option 3 - Mandatory security baseline)

Grade	Low Scenario	Central Scenario	High Scenario
Total average direct cost to manufacturers (2019 prices)	£49,953 in year one falling to £30,819 in year two	£54,227 in year one falling to £34,628 in year two	£58,140 in year one falling to £38,051 in year two
Estimated number of 'micro' manufacturers (year 1)	38	94	94
Aggregate direct cost to 'micro' manufacturers across the appraisal period (in PV terms, £m)	£11.0m	£30.2m	£33.1m
Estimated number of 'small' manufacturers (year 1)	19	47	47
Aggregate direct cost to 'small' manufacturers across the appraisal period (in PV terms, £m)	£5.5m	£15.1m	£16.5m
Aggregate direct cost to 'micro' & 'small' manufacturers across the appraisal period (in PV terms, £m)	**£16.5m**	**£45.3m**	**£49.6=m**
Total direct cost to retailers (2019 prices)	£3,907	£5,050	£6,538
Estimated number of 'micro' retailers	3015	3015	3179
Aggregate direct cost to 'micro' retailers (in	£10.6m	£13.7m	£18.7m

PV terms, £m)			
Estimated number of 'small' retailers	429	429	452
Aggregate direct cost to 'small' retailers (in PV terms, £m)	£1.5	£2m	£2.7m
Aggregate direct cost to 'micro' & 'small' retailers	**£12.1m**	**£15.7m**	**£21.4m**
Overall cost to consumers	**£28.6m**	**£61.0m**	**£71.1m**

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

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

233. DSIT has made best attempts to cover the full costs to small and micro businesses. There are some data limitations and DSIT will monitor the impact on small and micro businesses throughout implementation.

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

234. Business Population Estimates have been used to determine the distribution of UK consumer connectable product business sizes based on employment figures. However, in order to align with the updated definition of medium sized businesses (50-499 employees), which changed after research was conducted, DSIT assumes that half of the 'large businesses' in the Business Population Estimates fall in the category of 'medium businesses' as these have less than 500 employees. The splits of UK consumer connectable products businesses according to employee figures has been showcased below:

Manufacturers

- **Micro businesses** (0-9 employees) - 55% of businesses (94 manufacturers in the central and high estimate, 38 in the low estimate)
- **Small business** (10-50 employees) - 28% of businesses (47 manufacturers in the central and high estimate, 19 in the low estimate)
- **Medium business** (50-499 employees) - 13% of businesses (26 manufacturers in the central and high estimate, 10 in the low estimate)
- **Large business** (500 and above employees) - 5% of businesses (4 manufacturers in the central and high estimate, 2 in the low estimate)

Retailers

- **Micro businesses** (0-9 employees) - 87% of businesses (3015 retailers in the central and low estimate, 3179 in the high estimate)
- **Small business** (10-50 employees) - 12% of businesses (429 retailers in the central and low estimate, 452 in the high estimate)
- **Medium business** (50-499 employees) - 0.9% of businesses (37 retailers in the central and low estimate, 39 in the high estimate)
- **Large business** (500 and above employees) - 0.3% of businesses (5 retailers in the central and low estimate, 6 in the high estimate)

235. In order to estimate whether the impacts fall disproportionately on micro and small businesses, it would be necessary to calculate direct costs relative to expected micro and small business turnovers (see 8B(iii) - Do the impacts fall disproportionately on small and micro businesses?). For this estimation, the IoTUK database has been employed. 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.

236. Although the IoTUK turnover categories do not perfectly align with the EU definition of an SME, DSIT assumes that micro businesses have a turnover of less than £1m, small businesses have a turnover of less than £10m, medium businesses have a turnover between £10m and £50m, and large businesses have a turnover of over £50m. This split has been showcased below:

- **Micro businesses -** Turnover less than £1m
- **Small business -** Turnover between £1m and £10m
- **Medium business -** Turnover between £10m and £100m
- **Large business** - Turnover above £100m

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

237. It is possible that micro and small businesses will be disproportionately affected by the introduction of policy option 3 as the majority of direct costs identified by DSIT 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 'micro' and 'small' manufacturers relative to larger manufacturers, the turnover of an average manufacturer of consumer connectable products was estimated and compared to the expected turnover of a micro and 'small' businesses.

238. An estimate for average turnover was calculated using the median turnover between the turnover categories outlined above, 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 £36.6m compared to £0.3m for micro manufacturers, £1.7m for 'small' manufacturers and £17.7m for medium sized manufacturers.

239. For the central estimate of the preferred policy option, the overall direct cost to manufacturers in year one amounts to £54,227 per manufacturer (not including costs associated with the disposal of non-compliant goods), but falls to £34,628 from year two of the appraisal period in 2019 prices. In year one, direct costs amount to 0.15% of average manufacturer turnover and fall to 0.09% in year two. On the other hand, direct costs amount to 19.4% of micro manufacturer turnover and 3.3% of small manufacturer turnover, falling to 12.4% and 2.1% respectively (assuming turnover remains constant throughout the appraisal period). To be conservative, DSIT has assumed that all business sizes have the same disposal costs and therefore the burden is likely a large overestimate. This assumption has been made as there is a deficit of data.

240. The aggregate impact on 'micro' and 'small' manufacturers is calculated by multiplying the number of 'micro' and 'small' manufacturers by the average direct cost (note this does not include costs associated with the disposal of non-compliant goods). In the central estimate this amounts to £26.8m and £13.4m throughout the appraisal period respectively in present value terms.

Table 26 - Direct cost as a percentage of manufacturer turnover (Policy Option 3 - Mandatory security baseline)

	Low case	Central Estimate	High case
Total direct costs to manufacturers (2019 prices)	£49,953 in year one falling to £30,819 in year two	£54,227 in year one falling to £34,628 in year two	£58,140 in year one falling to £38,051 in year two
Average manufacturer turnover (2019 prices, £m)	£36.6m	£36.6m	£36.6m
Total direct costs to micro manufacturers (2019 prices)	£1,896,000 in year one falling to £1,169,569 in year two	£5,070,000 in year one falling to £3,237,751 in year two	£5,436,000 in year one falling to £3,557,770 in year two
Average micro manufacturer turnover (2019 prices, £m)	£0.28m	£0.28m	£0.28m

Direct cost as % of micro manufacturer turnover	17.8% in year one falling to 11% in year two	19.4% in year one falling to 12.4% in year two	20.8% in year one falling to 13.6% in year two
Total direct costs to small manufacturers (2019 prices)	£948,000 in year one falling to £584,784 in year two	£2,535,000 in year one falling to £1,618,875 in year two	£2,718,000 in year one falling to £1,778,885 in year two
Average small manufacturer turnover (2019 prices, £m)	£1.65m	£1.65m	£1.65m
Direct cost as % of small manufacturer turnover	3% in year one falling to 1.9% from year two	3.3% in year one falling to 2.1% from year two	3.5% in year one falling to 2.3% from year two
Direct cost as % of average manufacturer turnover	0.14% in year one falling to 0.08% from year two	0.15% in year one falling to 0.09% from year two	0.16% in year one falling to 0.1% from year two

241. Direct costs to retailers are expected to be lower and only occur in year one 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.

242. In the central estimate, there are 3,485 retailers of consumer connectable products within the UK, and it is estimated that 87% are micro businesses (3015) and 12.3% are small businesses (429). 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 £5,050 in year one with an estimated overall impact to micro retailers of £13.7m (£10.6m in the low scenario and £18.8mm in the high case scenario) and an estimated overall impact to small retailers of £2m (£1.5m in the low scenario and £2.7m in the high scenario).

243. 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 turnover[178], 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.

244. In the absence of this data, the market share held by businesses in the UK private sector with employees 0-49[179] (small/micro businesses) has been used as an indicator. To this end, DSIT estimates 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 £36.1m (£17m is the low estimate and £40.3m is the high case estimate). It should be noted that this is expected to be a one off cost and as mentioned above, is likely to be an overestimate as DSIT has assumed that all business sizes will face equal disposal costs.

245. The analysis shows that, in the absence of mitigations, there may be some organisations that exit from the UK market due to the burden of these regulations. DSIT has set out its approach to mitigations below in 8B(v) - Could the impact on Small and Micro Businesses be mitigated while achieving the policy objectives?.

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

[179] https://www.gov.uk/government/statistics/business-population-estimates-2019/business-population-estimates-for-the-uk-and-regions-2019-statistical-release-html

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

246. 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 3) rests on a mandatory security baseline being implemented for every consumer connectable product made available to UK customers. 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 network.[180] 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 legislation (preferred option) will directly leave a significant proportion of the market vulnerable to cyber threats. Moreover, exempting 'small' businesses will indirectly leave customers using devices that meet the baseline level of security more 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.

247. The department intends to implement a number of mitigations to support small and micro businesses in complying with this regime. The PSTI Act provides the enforcement authority with the flexibility to determine which penalty, if any, is appropriate for a given instance of non-compliance, and will take into account a number of factors when determining how to respond to non-compliance, including, in the early stages of the regime being actively enforced, the size of the business, and its ability to have adjusted its business practices to become compliant by the point at which the infraction occurred.

248. 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 to be mandated 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 or retailer. Third party 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.[181] 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.

249. In the event that evidence emerged suggesting that the consumer connectable products made available to UK customers by Small and Micro Businesses posed a lesser risk, it would be possible to adjust the scope of products covered by the regime, if the Government considered it appropriate. 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?

250. DSIT has 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.

---

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

181 Sabanoglu, T, 2020, Third-party seller share of Amazon platform 2007-2020

251. The department has considered the potential exemptions detailed in the RPC Small and Micro Business Assessment guidance.[182] The mitigations we currently plan on incorporating within our approach are detailed below.

- **Transition period -** As noted in Box 10 - Key details of policy positions underpinning the preferred intervention (Option 3), the Government is providing businesses with an appropriate grace period to adjust their business practices before the PSTI product security measures fully comes into force. A response from a DSIT commissioned business survey[183] suggests that a 12 month grace period would give businesses sufficient time to sell non-compliant stock, and the Government commenced a grace period of this duration on 29 April 2023. In this period, industry is able to review the full legislative text of the regime before it enters into effect. In the early stages of the legislation being actively enforced, the department will work with the appointed enforcement authority to take 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 -** DSIT 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 -** DSIT 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 threats.[184] 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 catalyse the development of these schemes will enable smaller businesses to mitigate fixed costs such as those associated with familiarisation.

8C - Analysis of the impact on medium businesses

252.

8C(i) - Number and distribution of businesses in scope of the regulation

253. Business Population Estimates have been used to determine the distribution of UK consumer connectable product business sizes based on employment figures. However, in order to align with the updated definition of medium sized businesses (50-499 employees), which changed after research was conducted, DSIT assumes that half of the 'large businesses' in the Business Population Estimates fall in the category of 'medium businesses' as these have less than 500 employees. The splits of UK consumer connectable products businesses according to employee figures has been showcased below:

Manufacturers

- **Micro businesses** (0-9 employees) - 55% of businesses (94 manufacturers in the central and high estimate, 38 in the low estimate)
- **Small business** (10-50 employees) - 28% of businesses (47 manufacturers in the central and high estimate, 19 in the low estimate)
- **Medium business** (50-499 employees) - 13% of businesses (26 manufacturers in the central and high estimate, 10 in the low estimate)
- **Large business** (500 and above employees) - 5% of businesses (4 manufacturers in the central and high estimate, 2 in the low estimate)

[182] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827960/RPC_Small_and_Micro_Business_Assessment_SaMBA___August_2019.pdf

[183] **RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.**

[184] https://www.gov.uk/government/publications/grant-programme-for-consumer-iot-assurance-schemes-202021

Retailers

- **Micro businesses** (0-9 employees) - 87% of businesses (3015 retailers in the central and low estimate, 3179 in the high estimate)
- **Small business** (10-50 employees) - 12% of businesses (429 retailers in the central and low estimate, 452 in the high estimate)
- **Medium business** (50-499 employees) - 0.9% of businesses (37 retailers in the central and low estimate, 39 in the high estimate)
- **Large business** (500 and above employees) - 0.3% of businesses (5 retailers in the central and low estimate, 6 in the high estimate)

254. In order to estimate whether the impacts fall disproportionately on medium sized businesses, it would be necessary to calculate direct costs relative to expected medium business turnovers (see 8C(iii) - Do the impacts fall disproportionately on small and micro businesses?). For this estimation, the IoTUK database has been employed. 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.

255. Although the IoTUK turnover categories do not perfectly align with the EU definition of an SME, DSIT assumes that micro businesses have a turnover of less than £1m, small businesses have a turnover of less than £10m, medium businesses have a turnover between £10m and £50m, and large businesses have a turnover of over £50m. This split has been showcased below:

- **Micro businesses -** Turnover less than £1m
- **Small business -** Turnover between £1m and £10m
- **Medium business -** Turnover between £10m and £100m
- **Large business** - Turnover above £100m

8C(ii) - Do the impacts fall disproportionately on medium sized businesses?

256. It is possible that medium sized businesses will be disproportionately affected by the introduction of policy option 3 as the majority of direct costs identified by DSIT 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 medium sized manufacturers relative to larger manufacturers, the turnover of an average manufacturer of consumer connectable products was estimated and compared to the expected turnover of a medium sized business.

257. An estimate for average turnover was calculated using the median turnover between the turnover categories outlined above, and multiplying the median turnover for each category by the proportion of manufacturers within each band to give a weighted average.

258. For the central estimate, the overall direct cost to manufacturers in year one amounts to £54,227 per manufacturer (not including costs associated with the disposal of non-compliant goods), but falls to £34,628 from year two of the appraisal period. In year one, direct costs amount to 0.15% of average manufacturer turnover and fall to 0.09% in year two. On the other hand, direct costs amount to 0.31% of medium sized manufacturer turnover falling to 0.2% from year two (assuming turnover remains constant throughout the appraisal period).

259. The aggregate impact on medium sized manufacturers is calculated by multiplying the number of medium sized manufacturers by the average direct cost (note this does not include costs associated with the disposal of non-compliant goods). In the central estimate this amounts to £7.3m throughout the appraisal period.

Table 27 - Direct cost as a percentage of manufacturer turnover

	Low case	Central Estimate	High case
Total direct costs to manufacturers (2019 prices)	£49,953 in year one falling to £30,819 in year two	£54,227 in year one falling to £34,628 in year two	£58,140 in year one falling to £38,051 in year two
Average manufacturer turnover (2019 prices, £m)	£36.6m	£36.6m	£36.6m
Total direct costs to medium manufacturers (2019 prices)	£517,000 in year one falling to £318,973 in year two	£1,383,000 in year one falling to £883,023 in year two	£1,483,000 in year one falling to £970,301 in year two
Direct cost as % of medium sized manufacturer turnover	0.28% in year one falling to 0.17% in year two	0.31% in year one falling to 0.2% in year two	0.33% in year one falling to 0.22% in year two
Direct cost as % of average manufacturer turnover	0.14% in year one falling to 0.08% from year two	0.15% in year one falling to 0.09% from year two	0.16% in year one falling to 0.1% from year two

260. Direct costs to retailers are expected to be lower and only occur in year one 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.

261. In the central estimate, there are 3,485 retailers of consumer connectable products within the UK, and it is estimated that 0.9% are medium businesses (37). Similar 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. In the central scenario, the total direct cost to retailers amounts to £5,050 in year one with an estimated overall impact to medium retailers of £0.2m (£0.1m in the low scenario and £0.2m in the high case scenario) in present value terms.

8C(iii) - Could medium sized Businesses be exempted while achieving the policy objectives?

262. The department does not consider that an exemption would be appropriate for medium businesses. This is because the effectiveness of the preferred policy option (policy option 3) rests on a mandatory security baseline being implemented for every consumer connectable product made available to UK customers. 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 reports 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 network.[185] As outlined above, it is estimated that medium businesses account for a sizable proportion of the consumer connectable product market. With this in mind, exempting medium businesses from the legislation (preferred option) will leave an important proportion of the market vulnerable to cyber threats. Moreover, exempting medium businesses will leave customers using devices that meet the baseline level of security more vulnerable to cyber threats through the network effect described above. To this end, exempting medium 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.

263. The overall risk-profile of consumer connectable products made available to consumers by medium 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

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

severity of that harm to consumers is the same regardless of the size of manufacturer or retailer. Third party 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.[186] Medium 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.

264. In the event that evidence emerged suggesting that the consumer connectable products made available to UK customers by medium businesses posed a lesser risk, it would be possible to adjust the scope of products covered by the regime, if the Government considered it appropriate. This would be done by Ministers, subject to agreement by Parliament. For more detail please see Section 5B - Description of preferred option.

8C(iv) - Could the impact on medium Businesses be mitigated while achieving the policy objectives?

265. DSIT has committed to taking proportionate steps to mitigate any disproportionate impact this legislation and its enforcement would have on medium businesses, without compromising the effectiveness of the legislation in meeting its objectives.

266. The mitigations DSIT currently plan on incorporating within the approach are detailed below.

- **Transition period -** As noted in Box 10 - Key details of policy positions underpinning the preferred intervention (Option 3), the Government is providing businesses with an appropriate grace period to adjust their business practices before the PSTI product security measures fully comes into force. A response from a DSIT commissioned business survey suggests that a 12 month grace period would give businesses sufficient time to sell non-compliant stock.[187] The Government commenced a grace period of this duration on 29 April 2023. In this period, industry is able to review the full legislative text of the regime before it enters into effect 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 medium businesses, when determining the most appropriate response to instances of non-compliance.
- **Information -** DSIT has produced multiple publications on its proposals as well as engaged and formally consulted with industry including medium 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 medium businesses in adjusting their business practice to comply with their duties will also be made available.

8D - Break-Even Analysis

267. 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 point[188] 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.

268. Using this approach, the estimated number of avoided incidents needed for the preferred policy option to pay for itself amounts to 454,000 over the 10 year appraisal period in the central estimate, which translates to an average of 45,000 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:

[186] Sabanoglu, T, 2020, Third-party seller share of Amazon platform 2007-2020

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

[188] 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"

- 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)[189] An estimate for the number of recorded incidents across the UK is 3,364,437.

269. Under the preferred option, there only needs to be a reduction in incidents by around 1.5% for this policy to break even. The option that is being taken forward, option 3, will have the largest reduction in incidents as it mandates the security baseline in relation to all new consumer connectable products supplied to UK customers. DSIT assumes that a number of these 3 million incidents involved the existence of insecure consumer connected products, but the exact proportion is unknown. These estimates also do not take into account the higher cost of a business being breached.

270. It is more likely that the mandatory security baseline will deliver a reduction in incidents as it mandates that manufacturers meet the minimum security baseline,therefore reducing the opportunity for cyber attacks enabled by vulnerabilities in consumer connectable products. A mandatory labelling scheme will likely deliver more benefits than a voluntary one, but it is difficult to say whether this will outweigh the increase in the number of incidents required to break even. DSIT expects that the 454,000 incidents for the mandatory security baseline is more achievable than the 304,000 incidents for the mandatory labelling scheme.

Table 28: Break-Even analysis - Number of avoided cyber crime incidents needed over 10 year appraisal period

	Low Case	Central Estimate	High Case
Voluntary Labelling Scheme	29,524	50,079	52,851
Mandatory Labelling Scheme	171,598	304,409	319,041
Mandatory Security Baseline	254,683	453,995	453,561

Non-monetised benefits

271. While DSIT 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.

272. 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 savings.[190]

273. 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 the manufacturer of adherence to minimum standard (both 19%).[191]

274. DSIT 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

[189] https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates

[190] https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf

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

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 2E - 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 [DSIT] 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[DSIT] to capture all the costs relating to such large scale attacks".

8E - Analysis of potential trade impacts

8E(i) - Policy Option 2 - Mandatory security labelling scheme

275. 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%).[192]

276. 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.

277. 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%).[193]

278. 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%).[194] As the numbers reflect changes for a five-year time horizon, the annualised numbers are negligible. This is also true for other sectors affected by the proposed regulations. Bilateral imports from the UK's key trading partners are estimated to only slightly decrease in all sectors affected by the regulation.

279. The above results show that this impact on trade would be minimal as the costs to suppliers aren't thought to be overburdensome to stop supplying the UK market, or to significantly shift the supply or demand of the market for IoT devices.

8E(ii) - Policy Option 3 - Mandatory security baseline

280. 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.[195] Furthermore, foreign suppliers are expected to amend their products to ensure they comply with UK regulation. 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

[192] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
[193] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.
[194] 132 European Commission (2019). Reflection on the Economic Modelling of free Trade Agreements. Chief Economist Note. Issue 2, 2019.
[195] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.

measures with the highest relative increase for smart electrical equipment (+1.52%), followed by smart computer and electronic products (+1.42%).[196] 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).[197] 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 two years the effects are expected to phase out over the longer-term, leaving UK exports largely unaffected.

281. 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.

282. As this PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 will apply in respect of Northern Ireland, DSIT has notified the European Commission via the process set out in the Technical Standard and Regulation Directive 2015/1535/EU. DSIT has also notified the World Trade Organisation (WTO) of these regulations under the Technical Barriers to Trade Agreement.

8F - Equalities Impact Assessment

283. DSIT as a public authority has a legal obligation to consider the effects of policies on those with protected characteristics[198] 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.

284. 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.

285. There is reason to believe that regulation to require manufacturers of 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.).[199] 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 technology.[200]
- Customers aged 75+ are the least likely to have checked for the minimum support period for devices (only 6% responded "Yes").[201]

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

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

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

[199] Ipsos "Consumer attitudes towards IoT Security" report.

[200] Ipsos "Consumer attitudes towards IoT Security" report.

[201] Ipsos "Consumer attitudes towards IoT Security" report.

- 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.[202]
- Those earning £35,000+ usually spend more time researching a product than those earning less than £35,000.[203]
- 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+.[204]

286. Furthermore, the policy, by providing a transparent route for external parties to report vulnerabilities, will help to protect consumers including vulnerable groups.

287. 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.[205]
- 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%).[206]

288. 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.[207] Thus, the aforementioned price increase may have a disproportionate impact on their spending money.

289. 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.[208] 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.[209] Furthermore, while small businesses make up a significant portion of businesses they are unlikely to own the majority of the market share.

8G - Assessment of impact on innovation

290. 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. DSIT recognises the important role consumer connectable products play in many people's lives as well as the opportunities they create for innovation.[210] 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.

[202] Ipsos "Consumer attitudes towards IoT Security" report.
[203] Ipsos "Consumer attitudes towards IoT Security" report.
[204] Ipsos "Consumer attitudes towards IoT Security" report.
[205] Ipsos "Consumer attitudes towards IoT Security" report.
[206] Ipsos "Consumer attitudes towards IoT Security" report.
[207] https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/agegroupashetable6
[208] Ipsos "Consumer attitudes towards IoT Security" report.
[209] See section 8A for more details.
[210] https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf

8H - Assessment on competition

291. Using the guidance from the Competition and Markets Authority,[211] the competition checklist needs to be applied to this policy. The four questions are:

- Will the measures directly or indirectly limit the number or range of suppliers?
- Will the measure limit the ability of suppliers to compete?
- Will the measure limit the suppliers' incentives to compete vigorously?
- Will the measure limit the choices and information available to consumers?

292. The policy may mean that some suppliers decide to not supply the UK with products, but this would be their decision. There is not a significant barrier to entry being introduced as part of this legislation as two of the three requirements can be amended after a product has been produced. Some industry experts have also indicated that some of the default passwords could also be changed after the goods have been sold. There are only 10% of devices that are noncompliant meaning there could only be a minor decrease in the number of suppliers as a result of this policy.

293. This measure will bring every supplier up to a baseline of cyber security with the default passwords measure. This will mean that the 90% of suppliers will not be able to differentiate from the 10% that currently do not have this feature. This however is a step in the right direction. Suppliers can still compete with other cyber security features and also other features that influence the purchase decision of an IoT device.

294. The measure will not limit suppliers' incentives to compete, in fact it should promote it. Now that suppliers will have to share their policies on vulnerability disclosures and security updates, this will mean that consumers of these technologies will have more information available before purchasing a product. Organisations such as Which? will also be able to use this information before recommending products. Currently it is very hard for consumers to make a fully informed decision on how long the product will be updated and maintained for, this will change with this measure.

295. The measure will not limit but improve the amount of information available to consumers. As mentioned at the start of this section, the number of suppliers may decrease if the 10% of non-compliant devices for default passwords decide to drop out of the UK market, however this will be a good step for consumer protections. There is also likely to still be enough devices available to make the market competitive even if the 10% drop out.

296. To summarise, whilst there could be a minor impact on the number of suppliers, this measure is unlikely to have any adverse impacts on competition. This measure will increase the information available to consumers and will protect consumers from poorly protected devices.

297. As mentioned in the above trade assessment, there may be some change in international competitiveness. UK manufacturers may become less competitive compared to international suppliers in the global market. This impact is only expected to be small and phase out over the next two years.

[211] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/460784/Competition_impact_assessment_Part_1_-_overview.pdf

Section 9 - Monitoring and evaluation

9A - Evaluation of objectives

298. 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).

299. As expressed in NCSC Statement 4 - the view of the UK's technical authority for cyber threats is that estimating the reduction in the 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 is the objective of this policy intervention, i.e. to reduce risk to consumers and the broader economy, therefore necessitates that the success of the intervention be monitored indirectly using proxy variables.

300. 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 of Practice, the ETSI EN 303 645 standard, 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

301. This secondary legislation impact assessment principally relates to the PSTI (Security Requirements for Relevant Connectable Products), that represents the preferred approach. As detailed in 5C - How the preferred option will be given effect, this instrument defines the:

- Conditions for deemed compliance with the initial three security requirements;
- Products to be excepted from the PSTI Act; and
- Requirements for the Statement of Compliance, including minimum information required and minimum retention periods.

302. It also introduces three security requirements for manufacturers of consumer connectable products made available to UK customers, using powers from the PSTI Act.

303. As detailed in Section 6 - Proportionality approach, the department expects that actions taken to address the policy objectives would result in a material impact on businesses, consumers and the broader economy. The analysis in this impact assessment explores how the powers introduced by the PSTI Act could be used to introduce a baseline level of security for consumer connectable products. Should these powers be used to introduce further security requirements then the evidence base will be expanded and future impact assessments produced.

304. The policy objectives that this impact assessment relates to are to improve the level of security in consumer connectable products with particular emphasis on the top three guidelines detailed in the DSIT's Code of Practice.[212] The preferred approach would mandate three initial security requirements based on these guidelines. The view of the NCSC on the proportionality of monitoring the initial security baseline is detailed in NCSC Statement 7.

NCSC Statement 7
Minimum security baseline monitoring challenges

[212] DCMS, 2018. Code of Practice for Consumer IoT Security.
https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

"The overall objective of the proposed [DSIT] 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".

305. Considerations to be aware of and which may affect the success of the intervention includes 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 regime.
- **A short term increase in the number of insecure devices purchased.** There is a risk that leading up to the regime coming into force, i.e. during the transition period, retailers are likely to sell non-compliant products or products that would otherwise be non compliant 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.

306. Where appropriate, such as to address new threats, the Government has the power to introduce new security requirements through additional secondary legislation. Where future legislation introduced new security requirements, new impact assessments would be tabled alongside this legislation.

9C - Monitoring and Evaluation considerations

307. The department will seek to monitor the effectiveness of the chosen option through assessing compliance levels against the initial three security requirements. This will be done through:

- Using appropriate data from the appointed enforcement authority (OPSS) on variables related to compliance. This would likely include variables such as volume of reports of non compliance over time of reported and confirmed violations, and the results of market surveillance.
- The recurring assessment of existing external evidence regarding compliance, including the IoTSF and CopperHorse research series into vulnerability disclosure (for more detail see the publications and activity noted in 3E - Prevalence of baseline security measures); and
- The commissioning of bespoke research and/or evidence gathering activities, such as the collection of appropriate realised cost data, to assess levels of compliance both before and after the security regulations come into force to assess the impact of the regulations.

308. The department is already seeking to commission research regarding current compliance levels and the ongoing monitoring above will allow for future compliance levels to be assessed against this baseline and the current baseline values in this impact assessment. The department has funding allocated for the commissioning for future research over the next two years. This will allow for an objective evaluation of whether this regime has had a sufficient impact on making consumer connectable devices available to UK consumers more secure.

309. Additionally, the department will seek to understand the different vulnerabilities in consumer connectable products, and the risks and harms that can occur from a vulnerable consumer connectable product in order to assess whether the policy objective to reduce the risk to consumers, networks, businesses and infrastructure has been achieved. This will be monitored through:

- The commissioning of bespoke research and/or evidence gathering activities to explore the different threats to consumer connectable products, the harms that can occur from these products being compromised and whether the current security baseline mandated by the PSTI product security regime help to protect against these threats.
- Continued engagement with the NCSC and wider consumer group stakeholders to understand if and how consumer connectable products are being compromised.

310. The department will use all this information combined to monitor whether the security baseline mandated by the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023 is having the intended effect of reducing the risk to consumers or whether any further interventions are required with an interim review in 2.5 years. Whilst NCSC Statement 1 highlights that the currently proposed security requirements will have the biggest impact at the moment, this review will allow the department to understand whether the regulation continues to meet demands given the fast moving nature of cyber security.

311. The intended Enforcing Authority OPSS will monitor and report on its enforcement actions, specifically in relation to the notices issued as set out in the PSTI Act (compliance notices, stop notices and recall notices), the sanctions applied on economic actors (forfeiture, variable monetary penalties or possible criminal offences for failure to comply with corrective notices, obstruction of the Enforcing Authority, or impersonating enforcement officers) and also wider information relating to operational enforcement actions.

312. The exact format of any monitoring and reporting will be agreed as part of a Memorandum of Understanding between DSIT and OPSS. OPSS provide similar reports for other legislation that they enforce and information will be shared with DSIT or published as part of a report on Gov.UK as per their departmental processes.

Annex 1 - Top three consumer connectable product security guidelines

Annex 1A - Guideline 1 - No universal default passwords

313. Passwords are an easily-implemented, low-cost user authentication mechanism. Many consumer connectable products will use a password, with possible permutations of default usernames and passwords could include “admin/admin”, “admin/0000”, “user/user”, “root/12345” and “support/support”.[213] When a universal default or easily guessable default password remains unchanged when a device is in use and connected to a network, they can facilitate unauthorised access to the device. Such practice brings significant risk to consumers’ privacy and online security, particularly when the password of all devices of the same type are discovered and publicly disclosed by malicious actors..

314. 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.

315. This problem dates back years with some 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”.[214]

316. A 2017 Keeper Security survey[215] found that nearly three in four millennials in the 25-34 age range are not even aware that these devices arrive from most manufacturers with simple, pre-set default passwords. Some 65% of these millennials, who are the most active buyers of IoT devices, are not aware of the rising tide of concern around IoT device security.[216]

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

317. 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.

318. Although some vendors may seek to identify and remediate vulnerabilities before their devices and services are brought to market, testing for everything is impossible, and new vulnerabilities may emerge over the lifespan of the product. 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.

319. 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.

320. 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.

321. 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 of these schemes 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.

---

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

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

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

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

322. 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 Telecommunications and Information Administration survey[217] 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.

323. 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 and the adoption of consumer connectable products overall.

Annex 1C - Guideline 3 - Security updates

324. 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.

325. 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).

326. 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.[218] 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.

327. 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.[219] Even though this exposes them to higher risk of compromise from cyber criminals or other hostile actors.

[217] https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

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

[219] Ipsos Mori survey report

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

328. Following the publication of the Code of Practice for Consumer IoT Security (see the preceding section 3D - 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.

329. 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 14 below.

Box 14 - 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 1 - Voluntary security labelling scheme (Do-minimum option)*
- *Option 2 - Mandatory security labelling scheme (Other viable option)*

Preferred option

- *Option 3 - 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

330. 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 - 3E(i) - Progress in eliminating Universal Default Passwords, a recent Ipsos MORI report commissioned by DSIT 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.[220] This implies that there may be more devices on the market with default passwords than the available evidence suggests.

331. 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.

332. 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 limited user interfaces, the lack of settings for changing passwords or administering security updates, and limited support provided by manufacturers. In their 2019 investigation into wireless security cameras[221], Which? were unable to obtain a response from multiple manufacturers when security issues were found.

333. Without manufacturers providing clear information about security update provision, 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 problem[222]. 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 15 - 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.[223]

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.

334. The lack of progress in improving the cyber security of consumer connectable products (see the preceding section - 3E - 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 practices through increased consumer demand.

[220] 'Attitudes Towards IoT security'.

[221] https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/

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

[223] 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? https://osf.io/preprints/socarxiv/63zkt/

335. 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 without basic security measures in place, leaving consumers no choice but to buy products from manufacturers that do not adhere to the security guidelines in the Code of Practice, despite their higher levels of awareness.

336. Research has shown that price is most often the main consideration in the purchasing decision-making process for consumer IoT devices.[224] 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. Consumers may also still choose to purchase products with default user credentials that can be exploited by malicious actors to perpetrate significant harms to those users, other users, businesses, national infrastructure, or nation states.

337. Therefore, DSIT 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

338. 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.

339. Whilst the Government has introduced a new telecoms security framework[225] enabling 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 has a universal 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.

Annex 2A(iii) - Assurance schemes

340. 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 the security measures they have implemented.

341. The UK government has awarded grants to three companies to create assurance schemes for different consumer connectable product classes, providing industry with the opportunity to certify products against security standards, particularly ETSI 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.

342. 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

[224] Harris Interactive, 2019. Consumer Internet of Things Security Labelling Survey Research Findings.
[225] https://www.gov.uk/government/collections/telecommunications-security-bill

address the limited profit incentives for manufacturers to improve the security of their products in the first place.

343. 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, the PSTI product security regime has been designed to reflect the importance of assurance schemes in enhancing product security (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

344. In addition to the top three guidelines the initial security requirements mandated by the PSTI product security regime are based on , ten further security guidelines were detailed in the Code of Practice for Consumer IoT Security[226]. 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.

345. As detailed in the preceding section - 3D - Previous UK Government Interventions, these guidelines brought together what was widely considered to be good practice in IoT security, and were developed by DSIT and NCSC in collaboration with external cyber security experts, industry, academic institutions, and civil society organisations.

346. The option of legislating to immediately mandate a security baseline based on 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 16 for further details) and 2020 call for views on regulatory proposals in this space.[227, 228]
- 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 based on 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 and their associated harms, 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

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

[227] DSIT, February 2020, Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation

[228] DSIT, March 2021, Government response to the call for views on proposals to regulate consumer connectable product cyber security

to ensure compliance, as well as additional evidence gathering and analysis. It is therefore likely that an initial security baseline based on 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 based on the Code of Practice guidelines.

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

347. In May 2019, the Government launched a consultation[229] to gather feedback on policy options for improving the cyber security baseline for consumer Internet of Things (IoT) products.

348. This consultation ran from 1st May to 5th June 2019. A consultation stage impact assessment[230] 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.

349. 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.[231] A summary of feedback received on the consultation proposals is available in Box 16.

Box 16 - 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:

	Description	**Consultation Outcome**
Consultation Option 1	*Mandate retailers to only sell consumer IoT products that have an IoT security label (evidencing compliance with the top three Code of Practice guidelines)*	Carried forward for shortlist appraisal
Consultation Option 2	*Mandate retailers to only sell consumer IoT products that adhere to the top three guidelines of the Code of Practice*	Carried forward for shortlist appraisal
Consultation Option 3	*Mandate retailers to only sell consumer IoT products that have an IoT security label (evidencing compliance with the thirteen Code of Practice guidelines)*	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.

[229] DSIT, February 2020, Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation
[230] DSIT, May 2019, Secure by Design Consultation Stage Regulatory Impact Assessment
[231] 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

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 1 that the success of the labelling scheme outweighs the success of the core goal: to minimise the security risk of consumer IoT. Option 2, which would mandate retailers to sell only products that meet the top three code of practice guidelines, would go further in protecting customers from online threats."[232]

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 universal 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.[233]

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

350. 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.

351. Unfortunately, there were not enough responses to these questions to provide the level of evidence required for the final stage impact assessment. Consequently, DSIT 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[234] and 'Evidencing the cost of the UK government's proposed regulatory interventions for consumer IoT[235].

352. 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.

[232] DSIT, 2020. Government responses to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[233] DSIT, 2020. Government responses to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[234] CSES, 2020. Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape.
[235] RSM, 2020. Evidencing the cost of the UK Government's proposed regulatory interventions for consumer IoT.

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.

353. 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 3).

354. 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 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.

355. 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 introduction of any labelling option. Additionally, limited evidence was submitted as part of the consultation to suggest that a baseline based on the 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

356. To further augment the Government's policy development approach, and to gather additional external feedback on the option of mandating a security baseline, a call for views was launched in July 2020[236]. This sought feedback on proposals to regulate the cyber security of consumer connectable products by mandating a baseline based on the top three guidelines of the Code of Practice.

357. In March 2021, the Government published a response to the call for views[237], summarising the feedback provided, and outlining details of the Government's intended regulatory intervention (Option 3). 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 17.

Box 17 - 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

[236] DSIT, July 2020, Proposals for regulating consumer smart product cyber security - call for views
[237] DSIT, March 2021, Government response: Call for views on proposals to regulate consumer connectable product cyber security

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 based on 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

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 in and 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 2021[238].

Key feedback received	Key outcomes
Scope - inclusion of conventional IT products *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)*	*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*
Scope - overall scope approach *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.*	*Adoption of the policy approach proposed in the call for views*
Security Requirements *Broad support for the proposed security requirements (based on the top three Code of Practice guidelines), with additional feedback themes including an emphasis on the importance of the proposed intervention aligning with internationally agreed standards.*	*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.*
Obligations - placing obligations on distributors *Majority support for the distributors of consumer connectable products being obligated to play a role*	*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*

[238] DSIT, March 2021, Government response: Call for views on proposals to regulate consumer connectable product cyber security

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.	*Government committed to mandating that manufacturers ensure a statement of compliance accompanies in-scope products in the proposed intervention.*
Enforcement *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*	*Continued policy development aligned to the high-level approach included in the call for views*

Annex 2E - Development of labelling scheme options

358. To assist in the analysis of various labelling options, DSIT part-funded a survey study, conducted by researchers at the Dawes Centre for Future Crime at UCL between September 2018 to January 2019, to assess the influence of different (security-related) labelling schemes on consumer choice for consumer IoT products.[239] Further details of this study and its findings are presented in Box 18.

Box 18 - 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.

359. The findings of the Dawes Centre for Future Crime study (Box 18) 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.[240]

360. 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.[241]

[239] 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/

[240] 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/

[241] 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

361. 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.[242]

362. 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.[243] A link has also been identified between nutrition knowledge and label use.[244] Research on the proportion of consumers who use labelling information to make healthier food choices is summarised in Table 28.

Table 28 - 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-analysis of randomised studies. Obesity Reviews, 17: 201–210.	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%).
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 Labelling 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.

363. The available evidence suggests that food labels generally have a positive effect on consumers' food choices. However, the research detailed in Table 28 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.[245]

364. 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,[246] by helping to guide consumers towards important

[242] Effective approaches to environmental labelling of food products, University of Hertfordshire, 2010.

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

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

[245] Malam, Sally & Clegg, Sue & Kirwan, Sarah & McGinigal, Stephen. (2009). Comprehension and Use of UK Nutrition Signpost Labelling Schemes.

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

information.[247] 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.[248]

365. 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.[249]

366. 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.[250]

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

367. 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), the Waste Electrical and Electronic Equipment Directive,the Toy Safety Directive and the e-mark.[251]

368. As previously discussed, the efficacy of a label also depends on consumer awareness and the prioritisation of security when purchasing a consumer connectable product. DSIT 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 considered security features to be important in their decision-making process, above other factors such as brand reputation, customer reviews, privacy features and design.[252]
- 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.[253]
- 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.

369. 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.

370. 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.[254] 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).[255] 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

[247] 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.

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

[249] 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.

[250] 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

[251] https://www.mondaq.com/uk/product-liability-safety/731088/product-marking-and-labelling-in-europe

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

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

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

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

this online or in a showroom, and that *"online information was much easier to deploy as it could be updated remotely"*.[256]

371. 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.

372. 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.

373. 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 consumers[257], so an additional label may only be effective for consumers where security is already a priority or where they have prior cyber security knowledge.

374. 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 complacency and overconfidence in the security of their products.[258] 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.[259]

375. 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.

[256] 'Evidencing The Cost Of The UK Governments Proposed Regulatory Interventions For Consumer IoT', RSM, 2020.
[257] Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019.
[258] DSIT, February 2020. Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation.
[259] 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/4vxp2/

Annex 3 - Risks and Assumptions

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
That no new vulnerabilities will be more readily exploited	The push to remove default passwords may mean that hackers develop new capabilities to easily hack these devices	The legislation is not as effective as first thought.	Break even analysis	None
Trust in consumer products will remain the same	The IA has not assumed that there will be any growth in IoT devices due to this legislation or decrease.	That the legislation may not prove as effective as fewer people buy the devices.		
Number of consumer connectable products	Ofcom research report [260] and data from Statista on the number of smartphones[261]	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[262]	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[263]	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. DSIT is confident in this estimate.
Number of IoT products with non-compliant default passwords	Which? data	Inaccurate estimation of compliance rate	Costs	DSIT is confident in this estimate
Number of IoT products with information on security updates	Which? data	Inaccurate estimation of compliance rate	Costs	DSIT is confident in this estimate
Number of IoT products with vulnerability disclosure policies	IoT Security Foundation report	Inaccurate estimation of compliance rate	Costs	DSIT is confident in this estimate
Proportion of devices within each product category	RSM consumer survey [264]	Affects the benefits through the replacement rate.	Replacement rate	This estimate is based on commissioned research. Sensitivity analysis has not been

[260] https://www.ofcom.org.uk/__data/assets/pdf_file/0007/102004/Review-of-latest-developments-in-the-Internet-of-Things.pdf

[261] https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/

[262] https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030

[263] 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

[264] 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
				used because DSIT is confident in this estimate.
The likelihood of a cyber attack	The likelihood of a cyber attack resulting from insecure consumer connectable products has been 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. 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).	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. 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. DSIT 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 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 top three guidelines set out in the Code of Practice, as a proportion of UK manufacturers (170). In the worst case scenario the estimate is 0.39%.	Inaccurately estimating the benefits	Costs	In the central and optimistic scenario the estimate is 1.8% and in the worst case scenario the estimate is 0.39%.
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	Costs	Sensitivity analysis has been used around the central estimate. 10% in the worst case scenario and rising gradually. 51% in the optimistic scenario.

Assumption	Evidence	Risk	Relevant section	Sensitivity Analysis Undertaken
The proportion of devices sold with a 'positive label' under the mandatory labelling scheme scenario.	A DSIT assumption	Inaccurately estimating the benefits	Costs	Sensitivity analysis has been used and ranges from 13% in the worst case scenario to 50% in year two, 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	Costs	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[265] manufacturers and 3,485[266].	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 number of manufacturers 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 [267]	Inaccurately estimating familiarisation costs	Familiarisation costs	This is based on commissioned evidence. Sensitivity analysis has not been used here. DSIT is confident in this estimate
Average wages	RSM business survey [268]	Inaccurately estimating both self-assessment and familiarisation costs	Familiarisation costs and self-assessment costs	Sensitivity analysis has not been used here. DSIT is confident in this estimate.
Time spent on self-assessment	RSM business survey [269]	Incorrectly estimating the self-assessment costs	Self-assessment costs	Sensitivity analysis has not been used here. DSIT is 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

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

[266] https://www.statista.com/statistics/476698/uk-electric-household-appliances-retailers-by-employment-size/

[267] 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

[268] 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

[269] 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
				and central estimate to 21 in the worst case scenario.
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 1 due to a lack of available evidence. Evidence from the RSM business survey, 2020.	Incorrectly estimating the cost of 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 DSIT assume that 10% will be disposed of.	This is based on the estimated proportion of consumer connectable products in the UK with 'default passwords'.	Overestimate the costs	Disposal of non-compliant stock	Sensitivity analysis has been used here. 10% is the central estimate, 5% is the optimistic estimate and 45% is the worst case scenario.
Under the top 3 (policy option 3) scenario DSIT assumes 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	DSIT is 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	DSIT is confident in this central estimate. Sensitivity analysis has not been used.
Proportion of businesses that are 'micro', 'small', 'medium', or large	Business Population Estimates, 2022	Incorrect cost estimates on consumers and on micro, small and medium sized businesses	SAMBA	In order to align with the new definition of medium sized businesses, DSIT assumes that half of the large companies fall into the category of medium sized enterprises. Sensitivity analysis has been performed.
Average turnover of micro, small and medium businesses	IoT UK database	Incorrect cost estimates on consumers and on micro, small and medium sized businesses	SAMBA	DSIT is confident in this estimate.