Title: Draft Electronic Communications (Security Measures) Regulations

IA No:

RPC Reference No: RPC-DCMS-4474(3)

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

Other departments or agencies:

Impact Assessment (IA)

Date: 01/03/2021

Stage: Consultation

Source of intervention: UK government

Type of measure: Secondary Legislation

Contact for enquiries: Selorm Davoh
selorm.davoh@dcms.gov.uk

Summary: Intervention and Options

RPC Opinion: informal advice

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
£3188.4m	£3187.5m	£364.2m	Qualifying provision

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

The next generation of mobile and fixed telecoms networks (like 5G and full fibre) raise security risks as well as economic opportunities. The widespread deployment of 5G and full fibre networks is a primary objective of government policy. These networks will be the enabling infrastructure that drives future economic growth; their security is paramount and must be ensured to deliver the economic benefits.

The Telecoms Supply Chain Review, published by the Department for Digital, Culture, Media and Sport (DCMS) in 2019 and supported by the National Cyber Security Centre (NCSC), undertook a comprehensive review of the supply arrangements for telecoms critical national infrastructure. The Review's starting-point was a set of concerns about the provision of equipment for both 5G and full fibre networks – these were largely related to the overall quality of software engineering, under-investment in cyber security, and a growing dependence on a small number of viable vendors, including high risk vendors.

Telecommunications providers are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks. However, there can be tensions between commercial priorities and security concerns, particularly when these impact on costs and investment decisions. The flaws identified in the Review's report were the result of practices that may have achieved good commercial outcomes but resulted in poor cyber security.

The Telecommunications (Security) Act 2021 and subsequent secondary legislation will establish a new, robust security framework for 5G and full fibre networks to ensure providers design, build and operate secure and resilient networks, and manage their supply chains accordingly.

What are the policy objectives of the action or intervention and the intended effects?

The government aims to improve cyber security standards and practices across the telecoms sector through a new, robust security framework set out in the Telecommunications (Security) Act 2021 ('the Act')[1]. The government published accessible information on the objectives of the Act in its factsheets, available online[2].

The security framework applies to providers of public electronic communications networks and services[3], and consists of three layers:

1. Strengthened overarching security duties in primary legislation to take appropriate and proportionate measures to identify and reduce the risks of security compromises occurring, as well as preparing for the occurrence of security compromises and taking measures in response to compromises;
2. Specific security requirements in secondary legislation that set out the security objectives and actions that must be taken to meet the duties in primary legislation; and
3. Guidance in the draft code of practice that sets out detailed technical measures that certain providers can follow to meet their legal obligations.

The draft Electronic Communications (Security Measures) Regulations are therefore a vital part of the new framework. The draft regulations have been developed from detailed security analysis conducted by the NCSC that used a sophisticated threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[4]. An early draft of the regulations was published in January 2021 to gather industry feedback[5]. The draft regulations published for formal consultation alongside this assessment have been updated to account for that initial feedback. They propose to address the security risks facing public networks and services by providing appropriate and proportionate security requirements in law with which public telecoms providers must comply. Ofcom, as the independent telecoms regulator, will be responsible for monitoring and enforcing compliance with the statutory requirements.

The final regulations will be supported by a detailed draft code of practice that will be published by DCMS alongside this consultation. The draft code of practice is divided into three parts. The first part explains the purpose of the draft code and its position within the new framework. The second part follows the structure of the draft regulations. It explains the key concepts underpinning them, to help providers carry out the technical measures associated with particular legal requirements in the draft regulations. The third part of the draft code sets out specific technical guidance measures, as a series of actions that could be taken by providers to demonstrate compliance with their legal obligations.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

The options we have considered are relating to the specific security requirements that will be set out in secondary legislation. These options are:

- **Option 1 (Do nothing):** This option involves DCMS taking no action to address the security issues identified in section 1.
- **Option 2 (Do minimum):** DCMS works with NCSC and other appropriate industry bodies to produce (non legally binding) best-practice guidance for telecoms network and service providers.
- **Option 3:** The Act places high level security duties on providers, with no further draft regulations set out in secondary legislation. A draft code of practice is consulted on and final one published as guidance only for industry to follow and for Ofcom to take into account in ensuring compliance with legal obligations.

[1] https://www.legislation.gov.uk/ukpga/2021/31/enacted

[2] https://www.gov.uk/government/publications/telecommunications-security-bill-factsheets

[3] The telecoms sector is defined by section 151 of the Communications Act 2003 in relation to public electronic communications networks (PECN) and public electronic communications services (PECS).

[4] Summary of the NCSC's security analysis for the UK telecoms sector, January 2020

[5] Early illustrative draft of Electronic Communications (Security Measures) Regulations, January 2021

- **Option 4 (the Preferred Option):** The specific security requirements are set out in draft regulations. These are applied appropriately to providers of public telecommunications networks and services (PECN and PECS) in different ways, reflecting the different characteristics of network security compared to service security. Implementation is phased by date and by type of provider.
- **Option 5 (Implementation Plus):** The specific security requirements are set out in the draft regulations as in the preferred option but implementation is phased by date only; the guidance setting out a single set of implementation dates applying to all providers.

The total costs (EANDCB, NPV and break-even analysis) estimated for our preferred option are illustrative at this stage due to the exclusion of Tier 3 cost estimates. We received a limited survey response from Tier 3 providers meaning we are unable to accurately estimate the costs incurred by these providers. We plan to re-issue our cost survey alongside the public consultation to enable us to estimate costs to all Tiers. This survey will also update our cost estimates to reflect the updated draft regulations and the draft code of practice potentially leading to changes in our cost estimates.

		[N/a]		
Is this measure likely to impact on international trade and investment?		Yes		
Are any of these organisations in scope?	**Micro** No	**Small** Yes	**Mediu m** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** N/A	**Non-traded:** N/A	

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:**

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 : Rob Fontana-Revel *(Chief Economist)* Date: 4th January 2022

Summary: Analysis & Evidence

Policy Option 4

Description: The Telecommunications (Security) Act 2021 placing strengthened overarching security duties on public telecoms providers, followed by specific security requirements set out in secondary legislation and subsequent codes of practice to provide detailed technical guidance to certain types of provider.

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
2021	2022	10	**Low: - -4978.3**	**High: -2162.3**	**Best Estimate: -3637.6**

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	1150.2	128.7	**2162.3**
High	2660.1	290.7	**4978.3**
Best Estimate	1904.7	216.7	**3637.6**

Note: Our full economic assessment differs from the estimates of total net present social value, business net present value and net cost to business each year set out on page 1 which are shown in 2019 prices with a base year of 2020 to aid comparability with other policies.

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

The impact assessment conducted for the Telecommunications (Security) Act was unable to estimate costs to providers. This was due to a number of issues, including the need for providers to prioritise resources to mitigate the impacts of the COVID-19 pandemic meaning they were not able to return a structured survey on the impacts of the Bill. We subsequently assessed the impacts of both primary and secondary legislation through a survey to estimate the costs that businesses will incur implementing the early illustrative draft Electronic Communications (Security Measures) regulations published in January 2021.

The results of this survey highlighted the significant costs of implementing those early illustrative draft regulations and estimated these costs for the largest providers (those expected to fall into Tiers 1 and 2[6]). In summary we found that, over the impact assessment period, 2022 - 2031, Tier 1 and 2 providers:

- could incur one-off costs in a range from £1,090m to £2,520m in present value terms assuming that these costs are incurred by all providers over the years 2022 - 2026. If smaller providers incur one-off costs two years later this would reduce to £1,080m to £2,500m in present value terms.
- could incur average annual ongoing costs in a range from £85m to £215m per year in present value terms assuming that these costs are incurred by all providers from 2023 onwards. If smaller providers incur one-off costs two years later this would reduce to £80m to £200m per year in present value terms.

We have assumed that these costs are incurred early, over the years 2022 - 2026 in the totals above. This conservative approach assumes that operators implement the requirements straight away rather than smaller operators delaying implementation.

Within these estimates the absolute costs per provider vary significantly reflecting the range of size and types of businesses affected. The largest providers and those with significant network infrastructure incur the most significant costs.

[6] To ensure measures are applied proportionately, the government will define three tiers of telecom providers in an initial draft code of practice, which will be finalised via public consultation. Tier 1 is expected to include the largest national-scale telecoms providers, Tier 2 medium-sized providers and Tier 3 the smallest providers.

The total costs (EANDCB, NPV and break-even analysis) estimated for our preferred option are illustrative at this stage due to the exclusion of Tier 3 cost estimates.We received a limited survey response from Tier 3 providers so we are not confident that the data we have is an accurate representation of the true costs incurred. We plan to re-issue our cost survey alongside the public consultation and hope that further data from Tier 3 providers will allow us to estimate costs to all Tiers. This survey will also update our cost estimates to reflect the updated draft regulations and the draft code of practice potentially leading to changes in our cost estimates.

The survey also gathered data on familiarisation costs for all providers in scope of the draft regulations. We found that there will likely be significant familiarisation costs as providers get ready to embed the draft regulations into their business processes. However, these remain small in proportion to the total costs to business and total £3.7m - £4.9m for providers across all Tiers.

In addition to costs of implementing the draft regulations, we expect Tier 1 and 2 providers to incur costs in reporting compliance with the draft regulations and these costs will depend on the frequency and style of compliance reporting required. We have estimated these costs based on metrics for cost of compliance which we use as a proxy. These indicate a cost to Tier 1 and 2 providers of approximately £11.4m annually. However, these costs could change depending on Ofcom's final reporting framework.

Finally, Ofcom expects to incur costs associated with monitoring and enforcing industry compliance of £52.5m - £70m over the impact assessment period. As a result of the Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, having regard to the draft code of practice in their regulatory work. DCMS will also incur additional costs in providing administrative support for the Secretary of State under the new security regime. These are expected to total £0.8m - £1.4m over the impact assessment period.

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

Indirect costs to suppliers
We have estimated the direct costs to PECN and PECS providers of each regulation including regulation 7 regarding supply chain security. We do not separately estimate the costs to suppliers of any requirements that may be passed through by contractual or other means.

BENEFITS (£m)	**Total Transition** (Constant Price) Years		**Average Annual** (excl. Transition) (Constant Price)	**Total Benefit** (Present Value)
Low	Optional		Optional	**Optional**
High	Optional		Optional	**Optional**
Best Estimate				

Description and scale of key monetised benefits by 'main affected groups'
The new security framework will reduce the vulnerability of public telecommunications networks in the UK to cyber risks. The potential costs of a security compromise are broad; the framework will help harden the network against such incidents, and reduce security risks by reducing the impact of a cyber attack or network outage.

Estimates suggest that the cost of a security breach or cyber attack for a UK telecoms company could be anywhere in the range of £3,000 to £250m. We estimate that the total cost over the impact assessment period of security compromises for PECN and PECS providers is £4,480m, within a range of £2,800m - £6,850m. Within this estimate, we have assumed that, over the next ten years, there will be two severe incidents which reduce the share price of the affected provider, resulting in a loss of £120m per incident. The new security framework will reduce the cost impact of security compromises, reducing the total cost of security compromises. However, we

have not estimated the proportion of costs that would be avoided and have therefore not included these benefits in the NPV and EANDCB.

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

The legislation will support the growth of 5G and full fibre networks and services in the UK by ensuring the security of these networks and services. The widespread deployment of 5G and full fibre networks and services is a primary objective of government policy. These networks and services will be the enabling infrastructure that drives future economic growth. The security of these networks and services is in the UK's economic interest. If these networks and services are judged to be insecure, their usage and economic value will be significantly reduced.

We consider that the economic benefit arising from 5G use cases, where network and service security and resilience are considered a prerequisite to their adoption, is likely to be a key indirect benefit resulting from this legislation. We have not included these benefits in the impact assessment calculator. This is because doing so would require us to make an assumption about what proportion of benefits to attribute to the new telecoms security framework - we do not have any information on which to base such an assumption.

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

We have used estimates of costs from providers to estimate the total cost to business of the early illustrative draft regulations published in January 2021. There is a risk that the ultimate cost to business once the legislation is implemented may vary from businesses' best estimate at this stage.

It is also the case that:

- We do not know how providers will implement the guidance in the draft code of practice once it is in place or to what degree existing or planned security processes will be in line with the code.
- The implementation timescales for the draft code of practice were not finalised when we estimated costs and this is likely to be a key driver of costs.
- The draft code of practice will be reviewed regularly and will be updated as new threats emerge and technologies evolve. Any such review and consultation on changes could affect the costs to business.
- This impact assessment was prepared in the early Spring of 2021 based on the early illustrative draft Electronic Communications (Security Measures) Regulations published on 13 January 2021. It will be updated based on the current draft of the regulations and accompanying draft code of practice.

BUSINESS ASSESSMENT (Option 4)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
415.5	**0**	**415.5**	1821.0

Summary: Analysis & Evidence

Policy Option 5

Description: The specific security requirements are set out in the draft regulations as in the preferred option but within the draft code of practice, implementation concessions are not provided to smaller providers.

FULL ECONOMIC ASSESSMENT

Price Base Year 2021	PV Base Year 2022	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: N/A	**High: N/A**	**Best Estimate: N/A**

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	N/A		N/A	N/A.
High	N/A		N/A	N/A
Best Estimate	N/A		N/A	N/A

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

The impact assessment conducted for the Telecommunications (Security) Act was unable to estimate costs to providers. This was due to a number of issues, including the need for providers to prioritise resources to mitigate the impacts of the COVID-19 pandemic meaning they were not able to return a structured survey on the impacts of the Bill. We subsequently assessed the impacts of both primary and secondary legislation through a survey to estimate the costs that businesses will incur implementing the early illustrative draft Electronic Communications (Security Measures) Regulations published in January 2021.

The results of this survey highlighted the significant costs of implementing those early illustrative draft regulations and estimated these costs for the largest providers (those expected to fall into Tiers 1 and 2[7]). Within these estimates the absolute costs per provider vary significantly reflecting the range of size and types of businesses affected. The largest providers and those with significant network infrastructure incur the most significant costs. These costs are based on a 48 month implementation period for Tier 2 operators and we will need to gather further data from our reissued cost survey to understand the impact of a shorter implementation period on these operator costs. The lack of data and evidence on how Tier 2 providers will approach this option as well as the cost implications of their actions have meant that we have opted to provide a qualitative assessment for option 5 at this stage.

We received a limited survey response from Tier 3 providers so it is important to note that we are not confident that the data we have is an accurate representation of the true costs incurred. We plan to re-issue our cost survey and hope that further data from Tier 3 providers will allow us to estimate costs to all Tiers. This survey will also update our cost estimates to reflect the updated draft regulations and the draft code of practice potentially leading to changes in our cost estimates.

The survey also gathered data on familiarisation costs for all providers in scope of the draft regulations. We found that there will likely be significant familiarisation costs as providers get ready to embed the draft regulations into

[7] To ensure measures are applied proportionately, the government will define three tiers of telecom providers in an initial code of practice, which will be finalised via public consultation. Tier 1 is expected to include the largest national-scale telecoms providers, tier 2 medium-sized providers and tier 3, the smallest providers.

their business processes. However, these remain small in proportion to the total costs to business and total £3.7m - £4.9m for providers across all Tiers.

In addition to costs of implementing the draft regulations, we expect Tier 1 and 2 providers to incur costs in reporting compliance with the draft regulations and these costs will depend on the frequency and style of compliance reporting required. We have estimated these costs based on metrics for cost of compliance which we use as a proxy. These indicate a cost to Tier 1 and 2 providers of approximately £11.4m annually. However, these costs could change depending on Ofcom's final reporting framework.

Finally, Ofcom expects to incur costs associated with monitoring and enforcing industry compliance of £52.5m - £70m over the impact assessment period. As a result of the Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, having regard to the draft code of practice in their regulatory work. DCMS will also incur additional costs in providing administrative support for the Secretary of State under the new security regime. These are expected to total £0.8m - £1.4m over the impact assessment period.

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

We will estimate the direct costs to PECN and PECS providers of each regulation, including regulation 7 regarding supply chain security. We will not separately estimate the costs to suppliers of any requirements that may be passed through by contractual or other means.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional		Optional	Optional
High	Optional		Optional	Optional
Best Estimate				

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

The new security framework will reduce the vulnerability of public telecommunications networks in the UK to cyber risks. The potential costs of a security compromise are broad; the framework will help harden the network against such incidents, and reduce security risks by reducing the impact of a cyber attack or network outage.

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

The legislation will support the growth of 5G and full fibre networks and services in the UK by ensuring the security of these networks and services. The widespread deployment of 5G and full fibre networks and services is a primary objective of government policy. These networks and services will be the enabling infrastructure that drives future economic growth. The security of these networks and services is in the UK's economic interest. If these networks and services are judged to be insecure, their usage and economic value will be significantly reduced.

We consider that the economic benefit arising from 5G use cases, where network and services security and resilience are considered a prerequisite to their adoption, is likely to be a key indirect benefit resulting from this legislation. We will not include these benefits in the impact assessment calculator. This is because doing so would require us to make an assumption about what proportion of benefits to attribute to the new telecoms security framework - we do not have any information on which to base such an assumption.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5
• N/A		

BUSINESS ASSESSMENT (Option 1)

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

Contents

Key Terms

Term	Abbreviation	Available at
The Telecommunications (Security) Act *(primary legislation)*	The Act	DCMS
The Electronic Communications (Security Measures) Regulations 2021 *(secondary legislation)*	The draft regulations	DCMS
Telecommunications Security draft code of practice	draft code of practice	DCMS
The Telecommunications (Security) Act including the Electronic Communications (Security Measures) Regulations and the future Telecommunications Security draft code of practice	The new security framework	Factsheet on the new telecoms security framework
Public electronic communications networks	PECN	Section 151 of the Communications Act 2003
Public electronic communications services	PECS	Section 151 of the Communications Act 2003

1. Problem under consideration and rationale for intervention

What is the issue being addressed

1.1 The Telecoms Supply Chain Review (the 'Review') was launched in October 2018 with the aim of establishing an evidence-based policy framework for the telecoms supply chain, taking account of security, quality of service, economic and strategic factors. The Review was triggered by concerns about the provision of equipment for both 5G and full fibre networks.

1.2 These concerns were 'largely related to the overall quality of software engineering, under-investment in cyber security, and a growing dependence on a small number of viable vendors, including high risk vendors.'[8] These were combined with the view that if 5G and full fibre networks are going to deliver significant economic benefits, their deployment must be secure and resilient.

1.3 The Review recommended a new security framework with three components. These were:

- new Telecoms Security Requirements;
- establishing an enhanced legislative framework for security in telecoms; and
- managing the security risks posed by vendors.

1.4 The Telecommunications (Security) Act was introduced in November 2020 to take forward the legislative aspects of these recommendations and received Royal Assent in November 2021.

1.5 This impact assessment accompanies the draft Electronic Communications (Security Measures) Regulations ("the regulations"). The draft regulations set out the specific security requirements that must be met by all providers of public electronic communications networks and services. The draft regulations are at the core of the new telecoms security framework and will deliver effective and enforceable telecoms security.

5G and full fibre networks must be secure and resilient

1.6 The deployment of 5G and full fibre networks across the UK is a primary objective of government policy. The government ambition is to connect at least 85% of the UK to gigabit broadband by 2025. The UK also wants to be a world-leader in 5G, with a target for the majority of the population to be covered by 5G networks by 2027.

1.7 Increased reliance on these new networks will increase the potential impact of any disruption and means there is a need to reassess the current telecoms security legislation. Whilst 5G broadly comprises the same network components as 3G/4G, it involves some key differences which may change the risk profile of these networks.

1.8 These are set out in Box 1 which is an extract from the Review[9]:

[8] The Review, paragraph 1.3.

[9] The Review, paragraphs 2.11 - 2.15.

Box 1: 5G networks and security

5G networks will behave differently. In the short term, upgrades to the core will ensure that there is smooth handover and aggregation of capacity between 4G and 5G networks. In the longer term, new 5G use cases will require dedicated bandwidth and guaranteed service quality (using 'network slicing'). Much of this new functionality will be delivered by new software functions hosted in the core.

The functions within the core are becoming 'virtualised'. This is allowing them to be deployed as software applications on shared hardware, rather than each function running on its own dedicated hardware. This process is called 'Network Function Virtualisation' (NFV) and the computer platforms that are used are called 'Network Function Virtualisation Infrastructure' (NFVi). To ensure the different NFV applications run smoothly and independently, NFVi have special management software. The 'Management and Orchestration' (MANO) software can play a critical role in ensuring the security and resilience of the virtualised applications. Given NFVi and MANO will underpin the critical functions of the core, they must comply with the highest levels of security.

Sensitive functions will move towards the 'edge'. Mobile core functions may move from centralised locations to local aggregations sites (i.e. to data nodes in metropolitan areas but not to each individual base station), which are closer to end-users, in order to meet the requirements of 5G applications for high bandwidth and low latency. Critically, as you push core functions closer to the edge of the network, it will also be necessary to push out the security services that support and protect them.

Different deployment models. 5G networks can be deployed in two ways: standalone (SA) and non-standalone (NSA). SA deployments are separate 'greenfield' networks that may share transport, routing and switching with the existing 4G networks. SA deployments are required to deliver the full functionality of 5G, such as ultra-reliable, low latency enterprise services.

Critically, NSA deployments will be the first phase of 5G in the UK over the next few years and will rely on existing 4G infrastructure. For NSA deployments, 5G network equipment will need to be compatible with legacy network (i.e. 3G/4G) equipment. For this reason, UK providers will tend to use their current 4G vendors for 5G rollout.

1.9 Likewise, increasing reliance on full fibre broadband (or 'fibre to the premises' - FTTP) will make the security and resilience of these networks important.

1.10 This is explained in Box 2 which is an extract from the Review[10]:

[10] The Review, Paragraphs 2.19 - 2.22.

Box 2: FTTP networks and security

The increased speed and reliability of FTTP networks is likely to result in consumers and businesses becoming reliant on these networks for new services. There are a number of factors which have implications for the risk profile of these networks. These are set out below:

Greater dependency by consumers and businesses. For example, in addition to internet access and voice calls (including emergency calls), services such as TV, home security and other smart homes services will depend on broadband. As well as residential users, many businesses will migrate to full fibre. Symmetrical speeds and lower latency will enable more corporate systems and services to be hosted in the 'cloud' – this increases operational efficiency but also makes network availability and reliability imperative.

Role of the incumbent. Unlike mobile networks where there are four national networks, fixed networks have just two incumbent providers in Openreach and KCOM (in Hull) that together provide national coverage. These incumbents serve several essential functions like alarm systems, telemetry and control systems which will migrate to fibre. As smaller, sub-national, providers build their own market share in the business connectivity market, particularly for critical services, they will need to ensure they are providing the necessary levels of security and resilience.

Multiple networks and switching between networks. In the long run, we expect the majority of UK premises to have a choice of FTTP network. This will reduce the dependency on the incumbent networks. However, unlike mobile networks where end-users can relatively easily switch between providers in the event of a significant and sustained network disruption, switching between FTTP networks will require engineer visits and new customer premise equipment.

1.11 In conjunction with these technological changes, increasing day-to-day reliance on online connectivity and digital services makes businesses and households dependent on the underlying telecommunications networks. New technologies are expected to transform how we work, live and travel providing opportunities for new and wide-ranging applications, business models, and increased productivity. These include internet of things (IoT) devices, connected cars, augmented reality (AR) and virtual reality (VR) technologies.

1.12 Increased reliance on these new technologies will increase the potential impact of any disruption and means there is a need to reassess the security framework. In exceptional scenarios the criticality of telecommunications networks could be heightened. For example, the Covid-19 pandemic demonstrated the need for new full fibre networks to be secure and resilient to support national economic activity.

There are potential market failures in the security and resilience of telecoms markets

1.13 In January 2020, the NCSC published a report detailing the findings from their extensive analysis of the security of the telecommunications sector[11]. Upon completing the threat analysis, they found that the majority of the highest scoring attack vectors fitted into one of the following five categories:

- Exploitation via the provider's management plane[12]
- Exploitation via the international signalling plane[13]
- Exploitation of virtualised networks
- Exploitation via the supply chain
- Loss of the national capability to operate and secure our networks

1.14 The assessment finds that the evidence points to a telecoms sector that needs to improve cyber security practices.

1.15 Findings from the UK Cyber Breaches Survey 2020[14] show that the information and communications sector has, across each year of the survey, consistently stood out as more likely to identify breaches. 62% of information and communications companies surveyed identified breaches or attacks in the last 12 months, compared to 46% across all sectors.

1.16 While 'information and communication' is a broad sector, the telecoms sector targeted by this legislation sits within it, and the statistic shows a clear need for improvements in security. This is supported by further evidence that the global telecoms sector experiences a relatively high number of breaches, detailed in section Economic Impact - benefits below.

1.17 The Review identified four factors that mean that the telecoms market is not incentivising good cyber security. They are:

- 'Insufficient clarity on the cyber standards and practices that are expected of industry,
- Insufficient incentives to internalise the costs and benefits of security. Commercial players are not exposed to the full costs and consequences of security failures; security risks are borne by government, and not industry alone,
- A lack of commercial drivers because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality, and
- The complexity of delivering, monitoring and enforcing contractual arrangements in relation to security.'[15]

1.18 The first three factors relate to market failures that may prevent economically efficient decisions being made from a societal point of view. These are:

---

[11] Summary of the NCSC's security analysis for the UK telecoms sector, 2020

[12] The management plane of a network is where administrative activity takes place. It is the most powerful part of the network infrastructure; whether used for provisioning and configuration of new equipment, or making changes to existing infrastructure or services.

[13] All public telecoms networks connect to each other over signalling networks. These signalling networks allow provider networks to connect to each other, reach each other's services and ultimately allow users to communicate with each other.

[14] Cyber Security Breaches Survey 2020: Statistical Release

[15] The Telecoms Supply Chain Review, https://assets.publishing.service.gov.uk/government/uploads/system/uploadsattachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf, Page 13.

- ***Externalities***: An externality is a cost or benefit that affects a third party who did not choose to incur that cost or benefit. The risks posed to the security and resilience of networks could include cyber security threats, data loss and corruption and outages and disruptions in networks and services. When these risks materialise the impacts are felt by network providers and their customers but also by government and members of wider society (who may be affected through loss of services or communications). If industry does not bear the totality of these costs it does not have sufficient incentives to address them. The Review showed that at present good commercial outcomes can result in poor cyber security.
- ***Asymmetric and Hidden information***: Asymmetric or hidden information refers to characteristics that are less well observed or unobservable by one side of the market. Consumers and businesses do not have full visibility of the threat against them. When consumers and businesses are affected by security and resilience failures they may have a low awareness of the cause of the impact. In some cases a security breach can lead to a cyber attack or corruption of data that is not discovered by the user affected. However this does not mean it will not have a negative impact on the user affected. As a result, when consumers purchase network services they may not place a high value on security compared to other factors such as cost and quality[16]. The same is true of businesses: the Cyber Breach Survey 2020[17] found that only 15% of all businesses surveyed have reviewed the cyber security risks presented by their suppliers.

1.19 These market failures combined with the government's objective to promote the rollout of 5G and full fibre networks create a strong rationale for intervention.

What sectors/markets/stakeholders will be affected?

1.20 The Communications Act 2003 places certain responsibilities on providers of PECN and PECS. It defines the terms PECN and PECS in section 151[18].

1.21 The Telecommunications (Security) Act 2021 amends the Communications Act to apply new duties on providers of PECN and PECS. The final regulations will be made using powers granted to the Secretary of State by new sections 105B and 105D of the Communications Act 2003 (inserted by the Telecommunications (Security) Act 2021). The companies within scope are explored in more detail in section 6 under the heading 'Number and type of businesses affected'.

1.22 We also expect there may be impacts on suppliers to PECN and PECS providers, who are not directly in scope of the legislation but will be affected through requirements on providers regarding their third party suppliers.

[16]According to a 2017 PwC study: Protect.me, consumers do not consider telecoms to be a high risk sector when it comes to digital security. Telecoms was ranked 20th out of 27 sectors on a scale of digital risk. The survey was conducted in 2017, and PwC surveyed a nationally representative sample of 2,000 Americans over the age of 18.

[17] Cyber Security Breaches Survey 2020: Statistical Release: an annual survey commissioned by DCMS. It was a random probability telephone survey of 1,348 UK businesses and 337 UK registered charities from 9 October 2019 to 23 December 2019.

[18] Public electronic communications network: "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public".
Public electronic communications service: "any electronic communications service that is provided so as to be available for use by members of the public".

1.23 In addition to new requirements placed on providers, Ofcom will be impacted through resource requirements to carry out enhanced reporting and oversight duties[19].

Why is the government best placed to resolve the issue?

1.24 The responsibility for the management of security and resilience risks to UK telecoms is shared between the government, Ofcom and industry. Industry is currently responsible for taking appropriate measures to manage the risk to the security and resilience of their networks under the existing section 105A of the Communications Act 2003.

1.25 The Review found that there can be tensions between commercial priorities and security concerns, particularly when these impact on costs and investment decisions. Equally, the business models of vendors have not always prioritised cyber security sufficiently.

1.26 The Review found that the current level of protections put in place by industry are unlikely to be adequate to address the identified security risks and deliver the desired security outcomes. Consequently, the role of policy and regulation in defining and enforcing telecoms cyber security needs to be significantly strengthened to address these issues.

1.27 The new security framework was introduced to address these problems. The draft regulations deliver on the Review's recommendations by setting out the priority outcomes and actions needed to reach an acceptable baseline security standard across the telecoms sector.

[19] The impacts on Ofcom have been accounted for in the cost section of this impact assessment: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937142/FINAL__The_Telecommunications_Security_Bill_2020___The_Telecoms_Security_legislation_-_Acc.pdf

2. Policy objectives

2.1. The objective of the Telecommunications (Security) Act aligns with the DCMS Outcome Delivery Plan[20], specifically priority outcome 3. This is to 'increase growth through expanding the use of data and digital technology and increasing innovation, while minimising digital harms to the UK's economy, security and society'. The draft regulations will support the government in achieving this outcome by providing a security framework to contain unacceptable levels of economic and national security risk in the UK telecommunications sector. As organisations become more reliant on digital infrastructure, they must become more resilient to cyber threats. The draft regulations will help ensure businesses are incentivised to manage telecommunications security risks which will help protect economic activity and consumers.

2.2. The purpose of the Telecommunications (Security) Act is set out in the UK Telecoms Supply Chain Review report and is 'to ensure providers of PECN or PECS take appropriate and proportionate measures to prevent, remove or manage the risks posed to the security of networks and services'[21].

2.3. With regard to the new security framework, it is intended to:

- Provide strengthened overarching security duties for providers of electronic communications networks and services (PECN and /PECS as defined in the Communications Act) to ensure the adequate security of networks and services;
- Provide a new duty for Ofcom to ensure providers comply with their security duties, to enhance its existing powers in this area;
- Provide delegated powers to make draft regulations setting out specific security requirements to further define the priority actions to be taken by PECN and /PECS providers; and,
- Provide powers for the DCMS Secretary of State to issue codes of practice, setting out detailed technical security guidance to assist Ofcom and relevant PECN /PECS providers on how those providers might meet their new legal obligations.

2.4. The objective of the specific security requirements set out in these draft regulations is to ensure that public telecommunications providers securely design, construct and manage their networks and services to protect against threats. The requirements are general enough to be applicable in some form to all network and service providers aside from micro-businesses.

2.5. The codes of practice are the way in which DCMS will seek to demonstrate what good security practices look like in the context of the new duties, and will contribute to ensuring the security framework is targeted, proportionate and actionable. The scope of the codes' application to particular types of company will be set out within the codes themselves. The technical content of the initial code will be based on the NCSC's draft guidance containing technical security measures.

[20] https://www.gov.uk/government/publications/department-for-digital-culture-media-sport-outcome-delivery-plan/dcms-outcome-delivery-plan-2021-to-2022#c-priority-outcomes

[21] The Review, Page 36.

International policy context

2.6. The way forward the government proposes is specific to the UK's national needs for securing telecoms critical national infrastructure (CNI). However, the UK is not alone in seeking to provide requirements for basic security protections across its networks and services. Other countries are seeking to improve security through new laws and/or guidance to address common vulnerabilities:

- Australia has taken steps in the Telecommunication Security Sector Reforms 2017 (TSSR) to strengthen the requirements for better management of national security risks of espionage, sabotage and foreign interference. Most recently, in 2021, Australia introduced a Security Legislation Amendment (Critical Infrastructure) Bill that amends the Security of Critical Infrastructure Act 2018 to enhance the existing framework for managing risks relating to critical infrastructure.
- India has produced the Telecoms Security and Assurance Requirements (ITSARs) which set out technical measures to protect telecoms equipment and systems.
- The United States has taken steps to improve network and service security by drafting the security guidance for 5G cloud infrastructures which covers wide-ranging guidance to detect and prevent lateral movement, securely isolate network resources, and protect data in relation to 5G networks utilising cloud infrastructures.
- The Netherlands regulation for telecoms security sets out measures that apply to the critical parts of networks. These include safe configuration of technical equipment, physical and virtual infrastructure; monitoring of technical infrastructure; and security assurance on software and management services.
- Ireland's Electronic Communication Security Measures set out technical measures that will be given a legislative basis for enforcement.
- Germany has taken steps through the IT Security Act 2.0 (IT-Sig 2.0) which addresses component risks via a two-part assessment mechanism for telecom vendors seeking access to Germany’s 5G networks. This enables the German government to ban the use of critical components (including 5G equipment) by telecom providers on the basis of national security, and ban the use of all critical components provided by a manufacturer which has not proven itself to be trustworthy in severe cases. Also, further requirements have been placed through the Catalogue of security requirements which covers various potential risks and requires network operators and service providers to meet strict security requirements.

2.7. The way forward should therefore be seen in the context of the UK as a leader in a more general global shift towards securing public telecoms networks and services.

3. Description of options considered

3.1. The Telecommunications (Security) Act received Royal Assent on 17 November 2021 replacing provisions 105 A - 105 D of the Communications Act 2003. The options we have considered begin with a counterfactual scenario where the security of telecommunications networks and services are regulated under the Communications Act 2003 as it stood prior to the Telecommunications (Security) Act. This allows us to assess the impact of primary and secondary legislation together as it currently stands only. Therefore, the proposed alternative options are variations of a new telecoms security framework comprising up to three layers:

1. **Strengthened overarching security duties set out in primary legislation, namely the Telecommunications (Security) Act**. The Act will require providers of PECN and PECS to take appropriate and proportionate measures to identify and reduce the risks of security compromises occuring, as well as preparing for the occurence of security compromises.
2. **Specific security requirements set out in secondary legislation, namely the Electronic Communications (Security Measures) Regulations.** The Act allows the Secretary of State to make draft regulations to detail specific security requirements that providers must take.
3. **Codes of practice** - the Act provides the Secretary of State with the power to issue codes of practice to provide guidance on how certain telecoms providers could comply with their legal obligations.

3.2. The options we have considered are:

- **Option 1 (Do nothing):** This option involves DCMS taking no action to address the security issues identified in section 1 and retaining the pre-existing obligations in sections 105A to 105D of the Communications Act prior to the Telecommunications (Security) Act coming into force. This is the counterfactual option against which the incremental impact of all other options are considered.
- **Option 2 (Non regulatory option):** DCMS works with NCSC and other appropriate industry bodies to produce (non-legally binding) best-practice guidance for telecoms network and service providers.
- **Option 3:** The Act places high level security duties on providers, with no further draft regulations set out in secondary legislation. A draft code of practice is consulted on and a final one is published as guidance for industry to follow and for Ofcom to take into account in ensuring compliance with legal obligations.
- **Option 4 (the Preferred Option):** The Act places high level security duties on providers, and specific security requirements are set out in secondary legislation. These requirements are applied to providers of communications networks and services (PECN and PECS) in a way that is appropriate and proportionate, reflecting the different characteristics of network security vs service security. A draft code of practice is published as best practice guidance for industry to follow and for Ofcom to take into account in ensuring compliance with legal obligations.
- **Option 5 (Implementation plus):** The specific security requirements are set out in the draft regulations as in the preferred option but implementation is phased by

date only; this option sets out a single set of implementation dates applying to all providers.

Option 1: The 'Do nothing' option

3.3. The 'do nothing' option, or the status quo, is the continuation of current arrangements as if the intervention under consideration were not to be implemented. In this case, this refers to continuing with the security arrangements under sections 105A to 105D of the Communications Act 2003 prior to the Telecommunications (Security) Act.

3.4. We discussed in section 1 the problem under consideration and rationale for intervention. The 'do nothing' option would be to leave the previous existing framework under the Communications Act 2003 in place. However, the Review found that this was not adequate in addressing the threat assessment and that there were four reasons that the do nothing option is not workable. These are:

- 'Insufficient clarity on the cyber standards and practices that are expected of industry,
- Insufficient incentives to internalise the costs and benefits of security. Commercial players are not exposed to the full costs and consequences of security failures; security risks are borne by government, and not industry alone,
- A lack of commercial drivers because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality, and
- The complexity of delivering, monitoring and enforcing contractual arrangements in relation to security.'[22]

Options 2: Non Regulatory Option: Guidance

3.5. The Communications Act (2003) contained existing provisions in relation to the security of providers of communications networks and services prior to Royal Assent of the Telecommunications (Security) Act. It is therefore not possible to set out a non-regulatory option.

3.6. Option 2 considers a 'no additional regulation' approach. In this option additional guidance is created in place of the new security framework. This additional guidance is within the existing framework of the Communications Act (2003) prior to Royal Assent of the Telecommunications (Security) Act.

3.7. Since 2011, Ofcom has set out guidance on following the previous legal obligations contained in sections 105 A-D of the Communications Act 2003. The Review found this has not led to sufficient incentives to improve network and service security.

3.8. Under this option DCMS works with NCSC and other appropriate industry bodies to produce (non-legally binding) best-practice guidance for telecoms network and service providers.

3.9. However, since the Telecommunications (Security) Act has now received Royal Assent this option is not considered in detail. Option 3 sets out a guidance based option within the framework of the new Telecommunications (Security) Act.

[22] The Telecoms Supply Chain Review, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf, Page 13.

Option 3: Guidance issued within the new security framework

3.10. Option 3 considers the use of a draft code of practice providing guidance without the specific security requirements set out in secondary legislation, namely the Electronic Communications (Security Measures) Regulations.

3.11. The draft code of practice uses the framework set out in the updated Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021). The Act has created a new security framework via strengthened overarching security duties on public telecoms providers coupled with powers for the Secretary of State to make draft regulations and issue codes of practice.

3.12. This includes provision for the Secretary of State to create codes of practice giving guidance and for the draft code of practice to be taken into account by Ofcom.

3.13. Codes of practice can set out the detailed technical security measures that providers can take to meet their legal obligations. The Act requires the Secretary of State to consult on any codes, and the consultation on the first code - published alongside this impact assessment - includes options for its implementation such as the scope of application and timescales for implementation.

3.14. The first draft code of practice would be published by the government to demonstrate to certain providers how they can meet their legal obligations. The code would - as currently expected - contain the technical security guidance measures targeted at areas of specific vulnerability, based on threat analysis that takes into account real-world attacks, penetration testing results and NCSC threat modelling. Under section 105H of the Communications Act (as amended by the Telecommunications (Security) Act 2021, Ofcom must take into account the provisions of the code when carrying out its functions to assess and monitor providers' compliance with their security duties.

3.15. Since the draft code of practice is guidance, breaching the draft code of practice itself does not make a provider liable to proceedings. However, Courts and Tribunals must, if they consider it relevant, refer to relevant provisions in a draft code of practice, which is in force at the time, when determining whether or not a breach of the duties set out in the Act has occurred.

Option 4: Regulations and Guidance (the Preferred Option)

3.16. Under the preferred option, the Electronic Communications (Security Measures) Regulations will set out specific security requirements clarifying the priority security outcomes and the strategic actions that must be taken to achieve them. These requirements are intended to apply to all providers of public electronic communications services and networks (PECN and PECS) with a particular focus on network providers, who are responsible for the security of telecoms infrastructure[23].

3.17. As in option 2, codes of practice would then set out the detailed technical security measures that providers can take to meet their legal obligations. The draft code of practice sets out a three-phased approach to implementation of security measures, reflecting differences in implementation costs and complexity of those measures.

[23] While all providers are responsible for the security of telecommunications networks, service providers typically do not own or operate significant quantities of physical infrastructure. The security of physical infrastructure is a focus of a large part of the framework and therefore applies to network providers more than it does to service providers.

3.18. To account for the need to reflect differences in the relative size of public telecoms providers, the draft code of practice proposes that Tier 2 providers should be given an **extra two years (dates specified in brackets)** to implement the measures beyond each of the timeframes set out above. Proposed implementation dates for Tier 1 providers are:

- **31 March 2023 (2025)** - proposed completion of the most straightforward actions achievable with minimal resource allocations
- **31 March 2025 (2027)** - proposed completion of actions which require devotion of new resources and a degree of complexity
- **31 March 2026 (2028)** - proposed completion of actions that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions

Option 5: Regulations and Guidance: Implementation plus

3.19. Under the 'implementation plus' option, the framework would be identical to that proposed by the preferred option. However, this option proposes a single set of implementation timetables for the measures in the draft code of practice for both Tier 1 and Tier 2 providers. The proposed implementation dates are:

- **31 March 2023** - proposed completion of the most straightforward actions achievable with minimal resource allocations
- **31 March 2025** - proposed completion of actions which require devotion of new resources and a degree of complexity
- **31 March 2026** - proposed completion of actions that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions

3.20. The 'implementation plus' option differs from option 4, in that it will remove the additional two year grace period granted to Tier 2 providers which is proposed under the preferred option 4.

3.21. It is worth noting that the implementation timeframes will be set out in the draft code of practice and not in the draft regulations. The timelines contained within the draft code of practice will serve as guidance on when government expects providers to have met their legal obligations, and Ofcom will take account of the code when monitoring compliance with the new framework. Should these dates not be met and sufficient mitigations or explanations not be provided, Ofcom may then take enforcement action using its new powers under the Telecommunications (Security) Act 2021.

4. Rationale and evidence to justify the level of analysis

Assessing impacts and ensuring proportionality

4.1. DCMS undertook a survey of a sample of providers to understand the cost impacts of the early illustrative draft regulations that were published in January 2021. This survey is the source of the estimates of the costs to business we have made in this document, as we consider it to be the most accurate and up to date source of information. The draft regulations are an innovative threat-based system of security legislation and the impacts are specific to UK providers and the way they operate their networks today. As a result, this primary research is the best way to understand the direct costs to business, as it takes account of this innovative approach and within the UK context.

4.2. We issued a detailed survey on 28 January 2021 to a number of larger providers. It was a structured set of around 80 questions asking providers for information on the changes required to implement the new security requirements and the ongoing and one-off costs of implementation for each section of the draft regulations. It also included questions on familiarisation costs, method of compliance and potential benefits of the legislation.

4.3. The survey asked for the costs of compliance with the early draft Electronic Communications (Security Measures) Regulations published on 13 January 2021, taking into account draft guidance from the NCSC which they were asked to use as a proxy for the future draft code of practice. Respondents were provided with copies of the draft regulations and the draft NCSC guidance in advance.

4.4. For smaller providers, we issued a shorter survey of around 20 questions on 28 January 2021. This survey did not ask for cost impacts per section of the early draft regulations, but asked for overarching one-off and ongoing costs of implementation. It also included questions on the degree of current compliance, familiarisation costs and potential benefits of the legislation.

4.5. We issued the latter through the UK's trade body for internet service providers, the Internet Service Providers' Association (ISPA), and the Federation of Communications Services (FCS).

4.6. We received 21 responses to the survey, with a response rate of approximately 38% for the population of larger providers and 2% for smaller providers. In order to better understand how representative the sample is, we asked questions regarding the type of provider and primary industry classification and compared this to the available data on PECS and PECN providers. We used the output on costs as a proportion of turnover to estimate the potential scale of impact on total providers, taking the type of provider into account.

4.7. The surveys were issued two weeks after the draft regulations were published. Providers were given six weeks to respond. Smaller providers were given the opportunity to attend a workshop in the first week of the survey process to better understand the content of the early draft regulations and what it means for them. This was not extended to larger providers as they were involved in round table discussions in the weeks following publication of the early draft regulations.

4.8. Clarification interviews were undertaken in the four weeks after the survey closed to follow up with particular points where providers were not clear in their responses or their responses raised additional questions (such as citing significantly different costs to

those given by similar providers). We undertook 16 interviews, which were attended by a DCMS technical adviser to help validate the responses where needed.

4.9. DCMS is in the process of updating the survey alongside the consultation document with the aim of asking a similar set of questions whilst including additional questions to all providers within scope.

How will DCMS ensure proportionality once new powers are in place?

4.10. New legal obligations - via strengthened overarching security duties and accompanying specific security requirements - will represent an absolute minimum for what is required to ensure network security is adequate and risks to national networks are mitigated. Providers may seek to meet those in various ways but DCMS recognises that many providers may choose to follow the detail set out in a draft code of practice as targeted, actionable measures.

4.11. The new legal duties will be overseen and enforced by Ofcom. In performing their duties Ofcom must have regard, in all cases, to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed.

4.12. Following the introduction of the Telecommunications (Security) Act, DCMS has been engaging with industry on the contents of the subsequent secondary legislation. This engagement has included roundtable sessions with providers of all sizes and functions, as well as suppliers and cross-sectoral representative bodies, reflecting the full breadth of the UK's telecoms market. This engagement gave telecoms providers and other affected parties the opportunity to comment on the technical contents of secondary legislation, helping to ensure the requirements are operationally realistic. It included an open call for technical feedback lasting four weeks from the publication of the early draft regulations.

4.13. DCMS is now carrying out a consultation on both the secondary legislation and draft code of practice. This consultation will build on the work feeding into this impact assessment to understand the costs to business that will result from these measures.

4.14. Micro-businesses are proposed to be exempt from the draft regulations and draft code of practice.[24] The legislation could have a disproportionate financial impact on micro businesses for applying the requirements, whose networks and services present much less risk to UK connectivity. The disproportionate financial impact on micro-businesses would primarily come from higher relative fixed costs, limited in-house technical expertise and higher relative familiarisation costs.

[24] The definition of micro-entities used in the draft regulations and draft code of practice is that set out in the Companies House Act 2006.

5. Preferred option with description of implementation plan

How will the preferred option be given effect

5.1. The Telecommunications (Security) Act takes forward the government's commitments in the Telecoms Supply Chain Review to establish an enhanced legislative framework for telecoms security. The Act received Royal Assent on 17th November 2021. It introduces a stronger telecoms security framework. The framework consists of three layers:

- First, by amending the Communications Act 2003, the Act creates strengthened overarching security duties on public telecoms providers
- Second, to support the security duties, the Act will enable more specific security requirements to be set out in secondary legislation.
- Third, the Act provides the government with the power to issue codes of practice which will provide detailed technical security measures as guidance on how certain providers can meet their legal obligations.

5.2. The draft Electronic Communications (Security Measures) Regulations. that will be published alongside this impact assessment, containing the specific security requirements.

What will legislation seek to do?

5.3. The requirements contained within secondary legislation will include targeted action to ensure that public telecommunications providers take such measures as are appropriate and proportionate for the purposes of:

- identifying the risks of security compromises occurring;
- reducing the risks of security compromises occurring; and
- preparing for the occurrence of security compromises.

5.4. The specific security requirements set out in the draft regulations will be applicable to providers of PECS and PECN. Expected implementation timeframes for certain providers are set out in the draft code of practice with reference to guidance measures against the draft regulations.

5.5. DCMS expects to lay the final Electronic Communications (Security Measures) Regulations later in 2022, so as to allow the new security framework to commence in October 2022. The government plans to align the coming into effect of the draft regulations, the commencement of remainder of the provisions in clauses 1 to 13 of the Act and the coming into force of the initial draft code of practice on this date. This is to ensure that formal commencement is in line with a fixed point in the financial year, to assist business decision making.

How will the legislation work?

5.6. The draft Electronic Communications (Security Measures) Regulations set out the priority security outcomes for providers of PECN and PECS, and the actions that must be taken to achieve them.

5.7. There are 13 substantive draft regulations addressing different activities to mitigate threats to networks and services. Each Regulation sets out the expected security

outcomes and the actions that must be taken to meet them. A summary of each Regulation is detailed below in Box 3:

Box 3 - Summary of the draft Electronic Communications (Security Measures) Regulations[25]

Network architecture
The draft regulation contains requirements that focus on ensuring providers understand the risks of security compromises to network architecture, record those risks, and act to reduce them. The regulation requires that providers securely maintain networks serving the UK by ensuring a sustainable and critical level of security expertise and data and equipment are accessible from within the UK at all times.

The requirement is intended to ensure networks are securely designed, constructed, maintained and redeveloped.

Protection of data and network functions
The draft regulation contains requirements to protect network management workstations from exposure to incoming signals and the wider internet, and monitoring and reducing risks from incoming signals to the network or service. In addition, providers must act to secure customer-facing equipment that they supply as part of the public network or service. This includes provider-managed equipment such as SIM cards, routers or firewalls.

Protection of certain tools enabling monitoring or analysis
The draft regulation contains requirements to protect monitoring and analysis tools by ensuring that providers account for these location-related risks. The schedule in the draft draft regulations lists certain high-risk locations where security capabilities that monitor and analyse UK networks and services must not be located. Security capabilities must also not be accessible from those locations. Alongside this, providers must inform Ofcom of any non-UK located centres that carry out monitoring and analysis activity. They must explain how they are taking appropriate actions to apply the new telecoms security framework to those overseas centres.

Monitoring and analysis
The draft regulation contains requirements that centre on using monitoring and analysis tools to identify and record access to the most sensitive parts of the network or service (defined as ‘security critical functions’). This includes securely retaining logs relating to security critical function access for at least 13 months, as well as having systems to alert and prevent unauthorised changes to the most sensitive parts of the network or service.

Supply chain
The draft regulation contains requirements to put appropriate contractual arrangements in place that ensure lifetime product and service security. They also require that written plans are in place in the event that supply from a third party is interrupted. Where a third party

[25] This summary reflects the latest published draft

supplier given access to sensitive data is another network provider, that provider must take the equivalent steps as the primary provider it is supplying.

Prevention of unauthorised access or interference
The draft regulation contains requirements that include applying best practices such as multi-factor authentication and password protections for users who have the ability to make changes to security critical functions. Alongside technical solutions, providers should actively approve and be responsible for any users - including third parties - who are given access to administrative accounts.

Preparing for remediation and recovery
The draft regulation contains requirements that propose that providers hold copies of network and service information that would allow them to rebuild and maintain their operations. A copy must be retained within the UK. Procedures are also proposed that would enable providers to recover swiftly and intelligently from a compromise.

Governance
The draft regulation contains requirements that propose to assign board-level responsibility (or equivalent) for oversight of new governance processes. They set out how to put an organisational framework in place to manage security incidents from a business process perspective.

Review
The draft regulation contains requirements that propose at least annual reviews are conducted of the risks facing networks and services. Written assessments would provide a 12-month forward recommendation of the overall risks of security compromise.

Patches and Updates
The draft regulation contains requirements that include standardising best practices such as rapid patching aiming to fix any new vulnerabilities within 14 days of availability.

Competency
The draft regulation contains requirements that set out the ways in which personnel with responsibility for security should be competent in fulfilling providers' legal security duties.

Testing
The draft regulation contains requirements including the use of testing techniques that simulate real-world attacks, across a broad spectrum of possible vulnerabilities and targets within the network or service.

Assistance
The draft regulation contains requirements that ensure providers - on request - give assistance to other providers in addressing security compromises. This also includes enabling pooled threat intelligence by sharing information relating to security compromises with other providers, and with other relevant third parties.

Source: The draft regulations were published on GOV.UK in March 2022.

5.8. The Act gives the telecoms regulator, Ofcom, powers to monitor and enforce industry compliance with the duties in the Act and specific security requirements in the draft regulations. It places new obligations on public telecoms providers to share information

with Ofcom that is necessary to assess the security of their networks, including reporting duties in the event of a security compromise.

5.9. The Act provides Ofcom with a general duty to ensure providers comply with their new security duties. Ofcom will be responsible for monitoring compliance and will be given enforcement powers in the Act to take action where providers are not meeting their obligations. These new powers and responsibilities will enable Ofcom to:

- Proactively assess the security practices of telecoms providers
- Take action where security is, or is at risk of being, compromised
- Make information available to the government and, beginning two years after commencement of clause 11, provide annual security reports to the government.

5.10. Ofcom will monitor compliance with the final regulations using its new powers. Ofcom intends that this will include a proactive oversight regime requiring larger providers to submit information on their activities to the regulator. Alongside issuing information requests, Ofcom expects to issue assessment notices to support this oversight.

Does the approach to implementation enable sufficient flexibility?

5.11. The new telecoms security framework has been designed to balance certainty and clarity to providers on achieving good security with the flexibility to update elements as needed. The draft regulations will be reviewed in the Post Implementation Review which will take place in 2027. They may be updated on a more regular basis to reflect changes in policy in response to the emergence of specific new threats or to address security vulnerabilities identified through compliance reporting.

5.12. The draft code of practice will be reviewed regularly and will be updated as new threats and vulnerabilities emerge and technologies evolve. While the draft regulations contain the minimum steps that must be taken to ensure good security across critical networks and services, the detailed measures contained in codes of practice will act as guidance.

5.13. The framework allows for providers to take their own actions to improve security rather than follow the draft code of practice, provided they can demonstrate to Ofcom that they continue to meet the law. This ensures flexibility for innovation and lets providers secure networks and services in ways that are appropriate to them. We anticipate that providers will use this flexibility based on our survey of PECN and PECS.In particular, we found that more than 70% of those that responded said they would comply with the draft regulations ‘by implementing the requirements set out in the draft code of practice where possible but for some areas we will set out our own approach’. The remaining respondents indicated that they would adopt the guidance measures set out in the draft code of practice.

6. Monetised and non-monetised costs and benefits of each option (including administrative burden)

Limitations of the calculations and estimates

6.1. While this impact assessment brings together evidence from a number of sources, we would like to note there are a number of limitations to the cost analysis. The costs are based on responses to a survey issued by DCMS, which was largely disseminated through relevant trade bodies, although it was directly issued to some larger providers. For this reason, the process was not random and the sample is therefore unlikely to be representative.

6.2. In particular, there was a much higher response rate among the largest providers (those expected to fall into Tiers 1 and 2) than smaller providers (those expected to fall into Tier 3)[26]. The response rate compared to the estimated population is shown in Table 1.

Table 1: DCMS cost impact survey response rate by Tier

	Estimated response rate
Tier 1	100%
Tier 2	22%
Tier 3	2%

6.3. A number of further limitations of estimating costs based on survey data have been identified:

- There is likely to be a selection bias whereby those providers who responded are the providers who are incurring the highest costs.
- This is innovative legislation and providers may face uncertainty in estimating the costs they will incur. Some cost figures provided in the survey were caveated with the respondent noting this uncertainty.
- A number of questions in the survey asked respondents to select a cost range. Since the cost ranges provided were wide (e.g. £25m-£75m), the cost analysis in this impact assessment offers a wide gap between the low and high estimates.

6.4. Additionally, there remain some uncertainties around the code(s) of practice which give rise to shortcomings in the analysis:

- When we carried out the cost survey we didn't know how providers will implement the draft code of practice once it is in place or to what degree existing or planned security processes would be in line with the code.
- When we carried out the cost survey we had not yet set implementation timescales for the draft code of practice and these are likely to be a key driver of

[26] To ensure measures are applied proportionately, the government has proposed three tiers of telecoms providers in the draft code of practice.

costs. We asked providers to provide costs based on implementation timescales of 24 months and 48 months[27].

- The draft code of practice will be reviewed regularly and will be updated as new threats emerge and technologies evolve. Any such review could affect the costs to business.

6.5. There are also uncertainties in relation to the growth of 5G and full fibre networks. The rate of growth of these networks could impact the costs of implementing the draft regulations to the degree that these costs are related to the size of the network. This includes uncertainty in relation to the number of providers affected. New providers may enter the market as 5G and full fibre networks grow and we cannot know how the draft regulations will affect these networks now.

6.6. The figures presented in this impact assessment are based on the best available data and our best efforts to align this with the expected impacts of the proposed legislation. This impact assessment was prepared in the early Spring of 2021 based on the early illustrative draft Electronic Communications (Security Measures) Regulations published on 13 January 2021.

6.7. The one-off and ongoing costs in this impact assessment are estimated using data from the industry responses to the DCMS cost impact survey only. Other sources to support the cost estimates given in the survey were not available for a number of reasons.

- Firstly, this is novel legislation and there are no similar regulatory regimes currently in place in other countries with which to compare cost estimates.
- Secondly, the legislation is highly technical and contains a number of novel technical requirements. Without a detailed knowledge of the inner workings of the networks managed and services delivered by each telecoms provider, it is difficult to produce an accurate cost estimate for complying with the new framework.
- Finally, each provider has a different starting point in terms of network security, and DCMS does not have a clear understanding of which draft regulations each provider currently complies with. For these reasons, DCMS was not able to produce a cost estimate that was independent of the responses given by industry.
- For these reasons, DCMS was not able to produce a cost estimate that was independent of the responses given by industry.

6.8. Alongside this Consultation Stage Impact Assessment we are publishing a consultation on the draft regulations and accompanying draft code of practice. We have also published:

- an updated version of the draft regulations; and
- a draft code of practice including implementation dates.

6.9. These updates are likely to have an impact on the costs estimates set out in this impact assessment and alongside this consultation we are distributing an update to our cost impact survey. Revised estimates will be set out in the final stage impact assessment

[27] Although we are aware that some survey respondents used their own timescales based on what they considered to be a reasonable timeframe for implementation.

The costs and benefits of the proposed approach

6.10. The preferred policy option is to introduce the Telecommunications (Security) Act followed by the draft regulations setting out specific requirements on providers. To help providers to achieve these legal obligations, the DCMS Secretary of State will publish a draft code of practice containing detailed technical guidance measures.

6.11. DCMS has engaged extensively with industry and wider stakeholders, including a survey to understand the costs to business that will result from these measures. The findings of this survey are set out below alongside our estimates of the potential benefits of the Telecommunications (Security) Act.

What is the counterfactual

6.12. In the section 'Description of options considered' we set out the 'do nothing' option which is also our counterfactual. This means continuing with the existing security requirements under the Communications Act 2003.

6.13. Sections 105 A-D of the Act cover the '*Security of public electronic communications networks and services'*[28]. Section 105A sets out the following four requirements to protect security of networks and services:

- Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.
- Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.
- Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.
- A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

6.14. Our approach to estimating the costs of our preferred option estimates the incremental costs of the draft regulations set out in our preferred option through a one off survey to affected companies. These incremental costs are expected to exclude the costs that would be incurred under the counterfactual.

[28] Communications Act 2003, Section 105.

Economic impact - costs

6.15. In order to estimate the costs of the policy options presented we need first to estimate the **number and type of businesses that will be affected.**

Number of businesses that will be affected

6.16. The security requirements set out in the draft regulations apply to all public telecommunications providers except those who are classified as micro-businesses, whose scale poses much less risk to UK connectivity[29].

6.17. The government has proposed that the draft code of practice include three tiers with different compliance expectations and levels of Ofcom oversight for different types of public telecoms providers:

- **Tier 1** providers should be those where a security compromise has the most widespread availability impact, and damaging security, economic or social effects.
- **Tier 2** providers should be those medium sized companies whose compromise would nevertheless impact critical sector or regional availability with potentially significant security, economic or social effects.
- **Tier 3** providers should be the smallest companies in the market that are not micro businesses. While security compromises could damage end-user customers, small businesses who do not support CNI do not present systemic risks to national, regional or critical sector availability.

6.18. It is difficult to estimate the total number of public telecommunications providers operating in the UK telecoms networks.

6.19. Available information on PECN and PECS providers provided by Ofcom shows that:

- There were 123 providers who paid administrative fees to Ofcom and therefore have a relevant turnover of over £5m in 2020/21[30]
- There were 193 providers who had applied for Code Powers[31] under the Electronic Communications Code and are therefore on Ofcom's 'register of

[29] The definition of micro-entities used in the draft regulations and draft draft code of practice is that set out in the Companies House Act 2006.

[30] Providers who have paid Administrative fees to Ofcom under section 38 of the CA 2003 in 2020/2021 and therefore had a relevant turnover of over £5m in 2019. Ofcom's Notice of Designation defines 'Relevant Turnover' as "turnover made from carrying on any Relevant Activity after the deduction of sales rebates, value added tax and other taxes directly related to turnover". It also defines 'Relevant Activity' as "any of the following: a. the provision of Electronic Communications Services to third parties; b. the provision of Electronic Communications Networks, Electronic Communications Services and Network Access to Communications Providers; or c. the making available of Associated Facilities to Communications Providers". https://www.ofcom.org.uk/__data/assets/pdf_file/0032/195269/network-service-providers-admin-charges-2020-21.pdf

[31] Code powers enable providers of telecommunication services, subject to necessary planning requirements, to construct infrastructure on public land (streets), to take rights over private land, either with the agreement of the landowner or by applying to the County Court. It also conveys certain immunities from the Town and Country Planning legislation in the form of Permitted Development. Further information is available here: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/electronic-comm-code

persons with powers under the Electronic Communications Code' on 12 November 2020[32]

- There were 596 providers who had telephone numbers allocated to them under Ofcom's Number Management System on 12 November 2020[33]

6.20. These categories overlap as providers that pay Administrative fees may also have applied for Code powers and/or have numbers allocated to them. In total, there were approximately 750 companies on the three lists as of November 2020. Approximately 300 of these are micro businesses will be excluded from the scope of the legislation under the micro business exemption.

6.21. In addition to the companies included on these lists, there may be further PECN/PECS providers who have a relevant turnover of under £5m, do not have Code powers and do not have allocated telephone numbers.

6.22. DCMS is currently carrying out a survey of electronic networks and service providers in the UK to understand more about the number, size and activities of companies providing electronic telecommunications networks and services. The results of this survey will feed into our estimate of the number of providers in the final impact assessment.

Type of businesses that will be affected

6.23. Providers of PECN and PECS include many different types of business. The main categories of PECN and PECS are:

- Vertically integrated provider: owns network infrastructure and sells directly to consumers and business
- Infrastructure provider: owns and deploys infrastructure but wholesales this to end users via third parties, and has no direct contact with end user customers
- Wholesale reseller: resells wholesale services to other internet service providers
- Consumer reseller: resells wholesale services to consumers
- Business reseller: resells wholesale services to businesses

6.24. We expect that costs will vary across these different types of businesses with the highest proportion of direct costs incurred by those companies that own and operate their own infrastructure - vertically integrated providers - and the least by resellers who do not own any network infrastructure.

6.25. We do not have a breakdown of PECN and PECS by these categories and we anticipate that many PECN and PECS fall into more than one category. In the analysis that follows we use the data that we have on the number of businesses that have Code Powers to provide a proxy for those PECN/PECS that own or operate network infrastructure. This is likely to be an imperfect proxy but we consider it is important for our analysis to distinguish between different types of PECN and PECS including those who do not own network infrastructure and whose primary role is to resell telecommunications services.

[32] Providers who have applied for Code Powers under the Electronic Communications Code and are therefore on Ofcom's 'Register of persons with powers under the Electronic Communications Code', 12 November 2020. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/electronic-comm-code/register-of-persons-with-powers-under-the-electronic-communications-code

[33] Companies who have been allocated telephone numbers by Ofcom, as of 12 November 2020. https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/numbering/numbering-data

6.26. The new security framework will not directly apply to equipment vendors or managed service providers, though these entities will be impacted indirectly via new obligations on PECN and PECS providers to secure their supply chains[34].

6.27. The Telecommunications (Security) Act amends the Communications Act 2003, removing existing sections 105A-D and replacing them with new provisions to strengthen the regulatory framework. Sections 105A-D of the Communications Act 2003 currently apply only to providers of PECN and PECS, and the amendments in the Act will not change this. Therefore, private communications networks are not in scope of this legislation.

Direct costs

6.28. Direct costs are those which fall upon those directly accountable for compliance, are immediate and unavoidable ('first round') and are in the market being regulated.[35] Indirect costs are those costs that are not direct. This distinction is important because direct costs form the score for Business Impact Target and the metric 'Direct Costs to Business (Equivalent Annual)'. The following sections detail the direct costs to industry, Ofcom and DCMS. The costs incurred by industry are split into familiarisation costs, one-off and ongoing costs and compliance and reporting costs. The costs incurred by Ofcom and DCMS are detailed in the section entitled 'Monitoring costs'.

Familiarisation costs

6.29. There will likely be significant familiarisation costs as providers get ready to embed the draft regulations into their business processes. We note that all providers will incur familiarisation costs in reading and understanding the primary and secondary legislation. Tier 1 and 2 providers will also incur the costs of reading and understanding the draft code of practice.

6.30. When we undertook the cost survey, the draft code of practice had not yet been drafted, and we could not estimate the familiarisation costs associated with it. As a proxy we therefore considered the familiarisation costs associated with the draft guidance from NCSC's Telecoms Security Requirements, which has formed the technical backbone for the draft code of practice and therefore was a suitable proxy for the code at the point the survey was conducted.

6.31. We recognise that providers will also need to disseminate the requirements within their organisation in order to fully understand the impact on business processes as well as disseminating the draft code of practice more widely to staff in order to embed new processes into their business.

6.32. To gain a better understanding of the impact from the early draft regulations on affected businesses, providers were invited to complete a survey. This survey ran from 29 January to 12 March 2021. The survey received 8 responses from the providers expected to fall into Tier 1 (100% of the sample size), 7 responses from those expected to fall into Tier 2 (22% of the sample size) and 7 responses from those expected to fall

[34] Equipment vendors provide physical equipment for networks. Managed service providers offer active support and administration of given systems on a providers' premises. Equipment vendors may provide managed services, and vice versa.

[35] RPC case histories, Direct and Indirect Impacts, March 2019.

into Tier 3 (just below 2% of the sample size). The survey collected information on familiarisation costs, business activities, network architecture, monitoring and audit, supply chain, security, governance and testing impacts.

6.33. In order to estimate these familiarisation costs, we asked survey respondents to estimate what costs they will incur as a result of familiarisation (defined as the costs of reading and understanding new/amended regulatory requirements and guidance) in relation to both the draft regulations and a future draft code of practice. We also followed up respondents' answers in clarification interviews to understand whether the familiarisation costs estimated include substantial dissemination and training costs.

6.34. Respondents were asked to give their answers in terms of person hours and by job function (Legal, IT, Compliance and Other). This allowed us to more accurately estimate the total cost of familiarisation across all PECN and PECS by Tier using the Annual Survey of Hours and Earnings, as shown below.

6.35. The largest providers (those expected to fall into Tier 1) stated an average familiarisation cost of approximately 550 hours, with the source of these cost hours evenly distributed across legal, operational and other job functions. Those respondents expected to fall into Tier 2 estimated an average familiarisation cost of approximately 420 hours. We consider that familiarisation costs for Tier 2 providers without code powers may be lower than for providers with code powers, given that providers without code powers are likely to be providers of communication services (PECS) only. Not all sections of the draft regulations and draft draft code of practice apply to PECS providers. Therefore, we do not expect these providers to spend the same amount of time familiarising themselves with the legislation as those providers with code powers, to whom the draft regulations and draft code of practice are likely to apply to in full. However, we do not have clear evidence to support this assumption, so in our cost model we have assumed costs to be the same across providers with and without code powers. Costs for all Tier 2 providers were driven by operational and other job functions.

6.36. Smaller providers (those expected to fall into Tier 3) provided an average familiarisation cost estimate of 300 hours, which is predominantly driven by operational job functions. Again, we assume that all providers incur the same familiarisation costs. We also note that the sample size for respondents in Tier 3 is low; however as the findings are consistent with the results for larger providers we retain them as a best estimate. We will, however, seek to improve these estimates through our updated cost survey which will feed into the final stage impact assessment.

6.37. The wages for information technology and telecommunications directors are taken from the ONS' Annual Survey of Hours and Earnings[36]. The median is used as a best estimate, as it is believed to be the most representative wage (it is less skewed by outliers).

[36] ONS, Annual Survey of Hours and Earnings, Revised - Occupation SOC10 (4) Table 14.5a Hourly pay - Gross 2019.

Table 1: Wage per hour: Annual Survey of Hours and Earnings (2019)

	Hourly wage rate	Hours	Total wage cost	Total wage cost with 22% uplift for overheads
Job Title	Median		£ GBP	£ GBP
Tier 1 providers				
Legal	26.18	160 - 180	4,100 - 4,700	5,000 - 5,700
Operational (e.g. IT or network functions)	24.46	180 - 190	4,400 - 4,500	5,300 - 5,500
Other [37]	24.53	175 - 180	4,300 - 4,500	5,200 - 5,500
Total	-	510 - 550	12,800 - 13,700	15,600 - 16,700
Tier 2 providers				
Legal	26.18	80 - 140	2,100 - 3,600	2,500 - 4,300
Operational (e.g. IT or network functions)	24.46	130 - 170	3,100 - 4,200	3,900 - 5,100
Other	24.53	130 - 180	3,200 - 4,400	3,900 - 5,400
Total	-	340 - 490	8,400 - 12,200	10,200 - 14,900
Tier 3 providers				
Legal	26.18	60 - 90	1,600 - 2,200	1,900 - 2,700
Operational (e.g. IT or network functions)	24.46	110 - 120	2,600 - 2,900	3,200 - 3,500
Other	24.53	100 - 130	2,400 - 3,100	2,900 - 3,800
Total	-	270 - 340	6,800 - 8,500	8,000 - 10,000

6.38. Overhead charges of 22% are added to the wages, in accordance with Regulatory Policy Committee guidance on implementation costs[38] which uses Eurostat data on UK non-wage and wage costs to calculate this uplift.

6.39. Based on this data, we estimate familiarisation costs will be:

[37] Job functions stated under the 'other' category include; security operations, business operations, assessment project teams, procurement, chief information security officer, privacy supplier, risk officer, business continuity and event management, external counsel, compliance, audit, architecture, engineering, regulatory, systems specialists, network design and development, legal, sales, support and customer engagement.

[38] RPC guidance note on 'implementation costs', August 2019.

- £15,600 - 16,700 per Tier 1 provider.
- £10,200 - £14,800 per Tier 2 provider.
- £8,000 - £10,100 per Tier 3 provider.

6.40. We have tested these estimates using speed of reading estimates produced by Eftec[39] which finds that the average speed of reading a technical text is 50-100 words per minute. The statutory instrument which sets out the duties on providers at secondary legislation is approximately 2,500 words and the draft code of practice is roughly 22,000 words. Based on this, the average time spent reading the secondary legislation and draft code of practice is between 4 and 8 hours per person.

6.41. Based on 8 hours per person, the 550 hours of familiarisation time given by Tier 1 providers suggests that, on average, 69 people in each Tier 1 business will be reading the documentation. For Tier 2 providers with code powers, the estimate of 420 hours suggests 53 people will be reading the relevant documentation. These numbers approximately reflect anecdotal feedback given to DCMS about the number of persons reading the draft regulations in bilateral conversations with larger telecommunications providers in June 2020. For Tier 3 providers with code powers, the 300 hours estimate translates into 38 people reading the documentation. This is likely to be an overestimation as many Tier 3 providers are small businesses with less than 50 employees. However, smaller providers may require external input in reading and understanding the draft regulations where they lack internal expertise and this might imply higher wages per hour. We have therefore retained the estimate as it is.

6.42. We assume that familiarisation costs will be incurred during 2022 and 2023. The total estimated familiarisation costs incurred by all providers over the impact assessment period is shown in table 2.

Table 2: Total familiarisation costs for all providers

Familiarisation costs in net present value terms over period 2022-31, £m	
Central estimate	4.3
Low estimate	3.7
High estimate	4.9

6.43. Whilst our survey clearly defined familiarisation costs[40], during the clarification interviews we noted that the scope of familiarisation costs was wide. Due to the complexity of the draft regulations and the size of some affected businesses the costs of dissemination and training were interlinked with familiarisation and were significant.

Options Analysis: Familiarisation costs

6.44. Our current estimates of familiarisation costs are based on an estimate of the number of person hours required as a result of familiarisation (defined as the costs of reading and understanding new/amended regulatory requirements and guidance) in relation to both the draft regulations and draft code of practice. These estimates would apply to both

[39] EFTEC (2013), "Evaluating the cost savings to business from revised EA guidance – method paper"

[40] Defined as the costs of reading and understanding new/amended regulatory requirements and guidance.

options 4 and 5. However, they may be lower under option 3 where firms would only need to read and understand a draft code of practice and not also the draft regulations.

6.45. We can estimate the proportion of familiarisation costs that would be incurred as a result of the draft regulations and draft code of practice by considering their relative length.

6.46. The statutory instrument which sets out the duties on providers at secondary legislation is approximately 2,500 words and the draft code of practice is roughly 22,000 words. Based on this, the average time spent reading the secondary legislation and draft code of practice is between 4 and 8 hours per person; using speed of reading estimates produced by Eftec[41] which finds that the average speed of reading a technical text is 50-100 words per minute. This is made up of one hour reading the secondary legislation and seven hours reading the draft code of practice; this would translate into a reduction of approximately 10% of familiarisation costs under Option 3 if reading speeds can approximate relative familiarisation time for the draft regulations and draft code of practice.

6.47. However, the number of people reading and understanding the draft regulations and draft code of practice will also be a key driver of familiarisation costs. Our current estimates indicate that on average 50 - 70 people within a larger operator will read and understand the draft regulations and draft code of practice. In our updated survey we are seeking input from stakeholders on how they would implement the draft code of practice under Option 3; the outcome of this survey may help us to validate these estimates.

One-off and Ongoing costs

Survey Approach

6.48. In addition to familiarisation costs, PECN and PECS will need to make changes to their networks in order to comply with the draft regulations. These changes include:

- Changes that Tier 1 and 2 providers (including other providers that are designated in the future) will make in order to comply with the requirements set out in the draft regulations and the guidance contained in the codes of practice.
- Changes that other PECN and PECS providers will make in order to comply with the requirements set out in draft regulations.

6.49. As detailed in the section above Rationale and evidence to justify the level of analysis, DCMS undertook a survey of a sample of providers to understand the cost impacts of the early draft regulations in early 2021. The survey responses provide us with a view of the scale of the changes that providers need to make to implement the early draft regulations. The responses also inform our estimates for the costs incurred by providers as a result of such changes.

6.50. The survey split these costs into one-off implementation costs and annual ongoing costs, so we have separated these costs in the following analysis. One-off costs are the upfront costs that providers will incur in implementing the initial changes. Examples of one-off costs include the costs of re-architecting networks, moving critical functions to the UK, negotiating contracts with suppliers and deploying privileged access workstations. Ongoing costs are the costs that providers will continue to incur once the

[41] EFTEC (2013), “Evaluating the cost savings to business from revised EA guidance – method paper”

necessary changes are implemented. Examples include costs of regular security patching, ongoing storage of data, provision of regular training to staff and increasing permanent headcount to meet monitoring and audit requirements.

Survey Methodologies

6.51. The cost estimates provided by industry in the cost impact survey have been produced using a range of methods. Some providers noted this methodology in the initial survey response, with some undertaking gap analysis to assess the impact of the draft regulations on their business, and others noted that their expected costs have not been considered in detail and the estimates given are rough.

6.52. The survey did not include a question on the methodologies used to produce cost estimates so we do not have a full picture of how providers reached their cost estimates. However, we have since contacted providers to ask for further information on the methodologies used. Two providers confirmed that they estimated costs by comparing against the cost of implementation of similar historic compliance regimes, with adjustments made based on the scope of the requirements and their assumptions. We plan to include a further question on methodology in our updated cost survey; which is available alongside this consultation. This will help us to better understand the data we receive.

6.53. While the survey did not ask for the job titles of those providing the cost estimates, some providers shared these during clarification interviews. Of the ten respondents that did provide us with job titles, 8 cited the input of a senior member of the network security or architecture team (or similar). This gives us confidence that the cost estimates were produced using technical expertise and experience.

Survey parameters

6.54. When asking the providers to respond to our cost survey we set out the parameters on which responses should be based. Specifically, providers were asked to:

- refer to a version of the early draft regulations published in January 2021;
- have read understood the NCSC's draft telecoms security guidance (larger providers only);
- assume that implementation of the early draft regulations would be required in 24 months for the largest providers and 48 months for smaller providers. This timeframe was provided to give providers a frame of reference to assess impacts.

6.55. These parameters have now been updated as (subject to consultation) a new version of the draft regulations and a draft code of practice have been published. Furthermore, the draft code of practice includes proposed implementation timetables.

6.56. We expect that these changes will impact the costs estimated in this Consultation Stage Impact assessment as set out in the Limitations of the calculations and estimates section. These estimates will therefore be updated in the final stage impact assessment.

6.57. In particular, the changes could impact cost estimates because:

- Amendments to the requirement for UK-based monitoring and audit capabilities in draft regulations 4 and 5 of the January 2021 draft regulations could reduce costs for providers who currently offshore these functions;
- Removal of the requirement to retain international signalling data could reduce overall costs;

- The proposed implementation of the most straightforward measures within 6 months of formal commencement for the largest providers, could lead to increased cost estimates. Likewise, for other providers, the implementation of these measures within 30 months could have the same impact. However, we note that these measures are expected to be achievable with minimal resource allocations and any cost impact is therefore expected to be small.
- The proposed implementation of requirements that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions within 42 months for the largest providers, could lead to reduced cost estimates. Likewise, for other providers, the implementation of these measures within 66 months could have the same impact.

Costs incurred by Tier 1 and Tier 2 providers

6.58. In this section, we estimate the costs to Tier 1 and 2 providers of complying with the Electronic Communications (Security Measures) Regulations.

6.59. The survey asked for the costs of compliance with the early draft Electronic Communications (Security Measures) Regulations published on 13 January 2021 taking into account draft guidance from the NCSC which they were asked to use as a proxy for the future draft code of practice. Respondents were provided with copies of the draft regulations and the draft NCSC guidance in advance.

6.60. We received 15 responses from larger companies, whom we expect to fall into Tiers 1 and 2. We estimate that this sample constitutes nearly 40% of all companies that will fall into these Tiers.

One-off and ongoing costs: total and as a % of turnover

6.61. In order to accurately estimate costs for Tier 1 and 2 providers, we have taken two different approaches to estimating costs.

6.62. For Tier 1 providers, we have summed the responses given in the survey to give a total cost estimate. This is because all providers that we expect to be in Tier 1 completed the survey. Providers were asked to select a cost range for each section of the Statutory Instrument. To calculate the low and high estimates for each provider, we summed the lower and higher bounds of the cost ranges chosen for each section. The central estimate is the mid-point between these bounds.

6.63. For Tier 2 providers, around 22% of the estimated total population provided a response to the survey. In order to estimate the costs across all Tier 2 companies, we have used the costs provided by the largest providers (those expected to fall into Tiers 1 and 2)[42] to estimate the median[43] cost as a percentage of a total turnover. We used this approach to account for the fact that the costs incurred are likely to increase with the size of the company (an assumption which is backed up by the survey responses). We

[42] The cost as a percentage of turnover for Tier 1 and 2 is used because the sample size for Tier 2 alone is small and there exists a substantial variation between responses. Including Tier 1 responses produces a more stable estimate.

[43] The median figure, rather than the mean, is used to reduce the impact of outliers.

estimated the total turnover for the entire Tier 2 population based on data from FAME, a company information database from Moody's Analytics[44].

6.64. All providers expected to fall into Tiers 1 and 2 were given a more detailed survey which asked respondents to provide a breakdown of their cost estimates. Specifically, the survey asked providers to select a cost range for nine key sections of the draft regulations, split by one-off implementation cost and ongoing annual cost.

One off and ongoing costs: by business type

6.65. We analysed costs by business type by splitting the survey responses by providers with Code Powers and providers without Code Powers. As set out in the section 'Number and type of businesses that will be affected', we have used the list of providers with Code Powers as a proxy for those providers who own or operate network infrastructure.

6.66. The majority of respondents to our survey hold Code Powers including all of the largest providers. However, comparing the providers likely to fall into Tier 2 with the providers with Code Powers, we estimate that around 40% of those providers that will fall into Tier 2 do not hold Code Powers. Whilst we only received a small number of responses from providers without Code Powers, the responses we received were consistent with our expectation that providers without Code Powers are more likely to incur lower than average costs.

Survey results

6.67. Using the survey responses, we calculated the median one-off and ongoing cost as a percentage of turnover from larger companies who responded to our survey and whom we expect to fall into Tiers 1 and 2. We then split this data by companies we expect to fall into Tier 1 and Tier 2; for Tier 1 all companies responded so we were able to directly estimate the total one off and ongoing costs.

6.68. To estimate the costs of the companies we expect to fall into Tier 2, we have calculated the median cost as a percentage of turnover incurred by survey respondents. We then estimated the total turnover of those Tier 2 providers with code powers using turnover data from FAME, and applied the median cost as a percentage of turnover to this total. When estimating the costs incurred by providers who do not have code powers, we have assumed those providers will incur 25% of the costs incurred by providers with code powers. This assumption is based on survey responses from Tier 2 providers without code powers and is a conservative estimate.

6.69. The results are shown in Table 3 below.

[44] Fame | UK & Ireland Company Data | Bureau van Dijk (bvdinfo.com)

Table 3: Total one-off costs[45] and ongoing costs[46] for Tier 1 and Tier 2 providers

	Total costs in net present value terms over the period 2022 - 2031 (3.5% discount rate), £m		
	Low estimate	Central estimate	High estimate
One-off implementation costs	1090	1800	2510
Annual ongoing costs	100	160	230
Total costs incurred	**2090**	**3400**	**4810**

6.70. We estimate a wide range of costs from a low of £2.1bn to a high of £4.8bn. This range reflects the format of our survey which asked respondents to indicate their costs within broad ranges. This approach was based on an assumption that respondents would find it difficult to provide a point estimate of costs impacts. This approach was also supported by our qualitative interviews where respondents noted that there is a wide degree of variance in their estimates and in many cases that they did not have a point estimate for their costs and were only able to indicate the range of costs.

6.71. Our central estimate is the midpoint of the low and high cases[47]. The survey asked respondents to select a cost range; the lower bound informed our low estimate and the higher bound informed our high estimate. In order to better understand the estimates provided in the survey, we used the follow up interviews to ask where their actual costs lay within this range. The majority of providers suggested they did not know where their costs would fall within the range chosen and we consider that there could be a high level variance from their estimates to the true costs. Many noted that there was a high level of uncertainty in the costs they expect to incur. In the absence of any further evidence, we have used the midpoint of the survey responses as the central estimate.

6.72. For Tier 2 providers we have considered whether selection bias means that those providers that responded were those that would incur proportionately more costs. However, our assumption that providers with code powers will incur lower costs than those given in the survey should reduce any potential selection bias. Therefore, we retain the midpoint as our central estimate.

6.73. Our central estimate gives a total cost incurred by Tier 1 and 2 providers of **£3.5bn** over the next ten years in net present value terms. This is based on Tier 1 providers incurring one off costs over the years 2022 to 2026 and ongoing costs from March 2023

[45] We have assumed one-off costs are spread equally over the first 4 years of the impact assessment period, based on a 48 month implementation period. The actual implementation period will be determined following the draft code of practice consultation.

[46] We have assumed ongoing costs will be incurred in full in years 3 -10. In year 1, providers will incur no ongoing costs and in year 2 they will incur half of the annual ongoing cost. In the low case, we have assumed that ongoing costs will begin in year 3 at half cost and will reach full cost in year 4 onwards.

[47] The central estimate is not an exact midpoint for the aggregated costs due to the spread of one-off and ongoing costs over the ten year impact assessment period.

onwards. We assume that Tier 2 providers spread one off costs over an additional two years (six in total) and incur ongoing costs from March 2025.

6.74. We have conducted some sensitivity analysis on these costs to illustrate the impact of varying our assumptions. In a high cost scenario, we use the mean cost as a percentage of turnover given in the survey, rather than the median, to estimate the costs to Tier 2 providers who have not responded to the survey. The turnover and Code Power assumptions for providers remain unchanged. In this scenario, our central estimate gives a total cost incurred by Tier 1 and 2 providers of **£4.2bn** over the next ten years in net present value terms.

6.75. In a low cost scenario, we assume that Tier 2 providers without Code Powers incur costs that are 10% of the costs incurred by those with Code Powers, rather than the 25% assumed in the base scenario. The cost assumptions for providers with Code Powers remain unchanged. In this scenario, our central estimate gives a total cost incurred by Tier 1 and 2 providers of **£3.4bn** over the next ten years in net present value terms.

Range of Estimates

6.76. In order to scrutinise the costs provided by industry in more depth, we have considered the range of cost estimates provided to understand how they differ between providers. We consider it most helpful to compare costs as a percentage of turnover; since we consider that the size of the company is a driver of the costs.The costs of meeting the regulation are not fixed in relation to output. Variable costs are driven by the size of organisation as this drives the cost of change and the size of network as equipment costs can be proportional to size of network where applicable.

6.77. For Tier 1 providers, all responses produced a central estimate of one off costs between 1-10% of annual turnover, with most responses falling between 1-4% of annual turnover. There is less variation in the ongoing costs as a percentage of turnover. The range of central estimates is 0.2% - 1.2% of annual turnover, with most costs falling between 0.2% - 0.4% of annual turnover.

6.78. There are a number of factors that we believe could cause the variation in costs across providers:

- Different interpretations of certain requirements within the draft regulations and the draft code of practice. A number of differing interpretations have been identified in follow-up interviews led by DCMS and technical reviews led by NCSC. DCMS and NCSC are working with industry to clarify these areas of uncertainty.
- Different interpretations of survey questions. For example, some providers included the costs of removing high-risk vendor equipment which relate to the Telecommunications (Security) Act but not the early draft regulations which were the subject of our survey; others did not.
- Nature of company, type of activity and location. For example, providers who are not headquartered in the UK have, in general, estimated higher costs for the proposed requirements to hold UK-based capabilities to secure and maintain networks.

6.79. For Tier 2 providers, the central estimates for one-off costs as a percentage of turnover were significantly varied across providers, ranging from 0% to 35%. Central estimates for annual ongoing costs as a percentage of turnover per provider were slightly closer in

range, from 0% to 10%. We believe this variation is explained by the same factors affecting Tier 1 providers. The other key differentiator is whether or not they own and operate their own network. We have accounted for this variation in our analysis, using providers with code powers[48] (which gives them the ability to build telecoms infrastructure on public land) as a proxy for those who own their own network infrastructure. In our cost models for providers in Tiers 2 and 3, we have assumed that providers without code powers will incur 25% of the costs incurred by providers with code powers.

Types of costs

6.80. Our central estimate sets out significant costs which reflect the width and breadth of the draft regulations as well as the number of providers affected. Box 3 - Summary of the draft Electronic Communications (Security Measures) Regulations sets out a summary of the content of the draft regulations and the key impacts on providers. The summary highlights that the draft regulations are broad, affecting providers in a range of areas from network architecture to governance and supply chain management.

6.81. The draft Electronic Communications (Security Measurements) Regulations have been developed from detailed security analysis conducted by the NCSC that used a sophisticated threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[49]. The draft regulations aim to address the security risks facing networks and service providers. In fact, our survey found that providers already considered that they met a large number of the requirements. When asked:

> *'Which of the measures detailed in the draft security requirements to be contained in secondary legislation do you already comply with?*';

all respondents chose between a quarter and three quarters of requirements with the highest number saying they complied with three quarters of the requirements.

6.82. Given the degree to which the requirements in the draft regulations are already being met by providers, it should be considered that some of the costs that respondents have estimated, could be costs that the organisations could incur anyway as a part of existing or future business change. However, we note that during follow up interviews all respondents, when questioned, identified the costs that they identified as incremental to existing and planned programmes.

6.83. Reflecting the range of providers affected, the key cost drivers cannot be neatly summarised. On average, we found that Regulation 3 on network architecture, Regulation 4 on protection of data and network functions and Regulation 5 on monitoring and audit caused the highest one off costs and ongoing costs. These costs are likely driven by the breadth of these draft regulations but we also note that many

[48] The grant of Code powers is intended to assist persons that provide an electronic communications network and/or system of conduits. In particular, persons with Code powers may construct and maintain infrastructure on public land (streets) without needing to obtain a specific street works licence to do so; benefit from certain immunities from the Town and Country Planning legislation; and apply to the Court in order to obtain rights to execute works on private land in the event that agreement cannot be reached with the owner of that land.

[49] Summary of the NCSC's security analysis for the UK telecoms sector

providers are affected by the need to apply the draft regulations to legacy equipment, requirements around customer premises equipment, the storage of data and data localisation.

6.84. The impact of the draft regulations and draft code of practice on legacy systems is an area of focus for the consultation accompanying this impact assessment. In particular we hope to understand whether the proposed approach addresses the risks posed by legacy systems and that a blanket approach to exempting specific systems would not be appropriate.

6.85. We also hope to understand, through our updated cost survey, where the impact of applying the draft regulations and draft code of practice to legacy systems is significant and what the scale of that impact might be. However, we recognise that the impact of legacy systems is likely to be different for every provider because the precise make-up and design of networks varies.

6.86. Tables 5 and 6 give a breakdown of the costs incurred per Regulation, based on the survey responses.

Table 5: One-off implementation costs split by Regulation

Section of the Regulations	***% of total one-off costs***
Network architecture	28%
Monitoring and audit	20%
Protection of data	18%
Supply chain	10%
Prevention of security compromise	9%
Remediation and recovery	7%
Governance & accountability	3%
Testing	3%
Competency	2%

Table 6: Annual ongoing costs split by Regulation

Section of the Regulations	***% of total ongoing costs***
Network architecture	17%
Protection of data	14%
Monitoring and audit	14%

Section of the Regulations	*% of total ongoing costs*
Prevention of security compromise	14%
Supply chain	11%
Testing	9%
Competency	8%
Remediation and recovery	8%
Governance & accountability	5%

6.87. It was also evident that respondents' estimates were subject to some uncertainty. In follow up interviews, respondents noted that there were areas of the draft regulations that they did not fully understand and this had required them to make assumptions to estimate costs. In addition, providers noted that there were some unknowns that could impact cost estimates; including the impact of passing requirements onto suppliers; uncertainty around legacy systems and security hardening of end user devices.

Costs incurred by Tier 3 providers

6.88. In this section, we set out the evidence we have gathered on the costs to the smallest providers (those that we expect to fall into Tier 3) of complying with the draft regulations.

6.89. Tier 3 telecoms providers will have a legal obligation to comply with the draft regulations and Ofcom will have a discretion to take action where a significant issue comes to its attention. While Ofcom will focus on oversight of Tier 1 and Tier 2 providers, Tier 3 providers may choose to adopt the measures included within the draft code of practice where these are relevant to their networks and services. This reflects the fact that while security compromises that affect a Tier 3 provider could damage end-user customers, small businesses who do not support CNI do not present systemic risks to national, regional or critical sector availability.

6.90. The cost impact survey issued by DCMS received a low response rate from those providers who we would expect to fall into Tier 3 at just under 2% of the total estimated population.

6.91. We issued the survey in January 2021 through ISPA, the UK's trade body for internet service providers, and FCS, an industry association for communications services providers[50]. We also ran a roundtable for ISPA and FCS members on 2 March 2021 to provide more context around the survey objectives and requirements. Following the initial dissemination of the survey to ISPA and FCS members, we received a response rate of just over 1% of the estimated Tier 3 population. In an attempt to increase the number of responses, we extended the survey deadline to 14 May and asked FCS and ISPA to specifically encourage those members that we expected to fall into the Tier 3 population to complete the survey. We also disseminated the survey through TechUK,

[50] Approximately 20% of the estimated Tier 3 population are members of ISPA or FCS.

the UK's technology trade association, on 28 April and encouraged TechUK members to complete the survey during a roundtable event on 7 May.

6.92. Despite these efforts, we received a total response rate of just under 2% of the Tier 3 population. This suggests a lack of engagement from Tier 3 providers with the legislation and its associated impacts. We do not have a clear picture of what is driving this lack of engagement. It may be that many Tier 3 providers consider that the legislation does not apply to them, which is a narrative that we are seeking to address through engagement with industry trade bodies. It is true that there are a wide variety of companies within Tier 3 and some will be impacted far more than others. Some providers offer local telecoms networks and thus will be affected by a number of the draft regulations; others simply package and sell third-party services, so are only tangentially impacted by the draft regulations. Some provide telecoms services as their primary activity; others provide telecoms services as a small proportion of their total operation. We do not have a complete picture of the types of providers that make up the market so the number that fall into each category is unknown. The premise that those providers who are more impacted is backed up by the survey responses; all 6 survey responses received were from providers with code powers. As noted in the Tier 2 cost analysis, providers with code powers are more likely to be those that own and operate their own network infrastructure and thus are likely to incur the highest costs.

6.93. Another possibility is that Tier 3 providers do not have the capacity to respond - there is a significant proportion of small and medium businesses in the Tier 3 population who are less likely to have a dedicated compliance team.

6.94. We hope to gather further views from Tier 3 providers during this consultation on the draft code of practice. We have also carried out a telephone survey of companies with activity in the Telecommunications SIC code; this survey should improve our understanding of the activities of businesses that will be affected by the new security framework including Tier 3 providers who may be less impacted by the requirements. We aim to use the outputs of this research to help us gather views from a wider cross section of Tier 3 providers and estimate the costs for all businesses in our final impact assessment.

Options Analysis: One-off and Ongoing costs

6.95. This options analysis considers the impact of Options 3, 4 and 5 on the one-off and ongoing costs that will be incurred by firms implementing the new security framework.

6.96. We consider the following potential impacts of options 3, 4 and 5:

- First, the impact of the draft regulations on how firms will implement the draft code of practice and how this might affect costs.
- Second, the **impact of implementation timetables** on one off and ongoing costs.
- Third, the **impact of implementation timetables on legacy equipment** and the extent to which legacy networks will be in scope of the draft regulations.

6.97. Overall, we consider it likely that the costs of option 4 (the preferred option) will be lower than option 5. The degree to which this is the case will depend on the incremental costs to providers of implementing change more quickly and the degree to which the longer implementation timetables in option 4 allow smaller providers to replace legacy equipment before requirements are applied to it. The costs of option 3 will depend on

how providers choose to implement the draft code of practice absent the draft regulations.

Impact of the draft regulations on how firms will implement the draft code of practice

6.98. In the survey that we carried out in January 2021, we asked providers 'How do you plan to comply with the draft security requirements to be contained in secondary legislation?', the options were:

- By implementing the measures set out in the draft code of practice
- By implementing the measures set out in the draft code of practice where possible but for some areas we will set out our own approach
- By implementing the measures set out in the draft code of practice in some cases but for the majority of areas we will set out our own approach

6.99. Over 80% of respondents said that they planned to set out their own approach for some or the majority of areas, with the majority choosing 'some' areas. The reasons given for this were:

Q2.3b - Please select the reason(s) for this approach.		
#	Answer	% of respondents
1	Difficult to implement requirements set out in the draft code of practice due to legacy systems	58%
2	To be more cost-effective	67%
3	To maximise network security	58%
4	To align with our company's global approach	42%
5	We prefer another approach, please explain	67%

6.100. The responses indicate that providers are likely to depart from the draft code of practice where they are able to do this. The response also indicates that providers expect to have lower costs by not complying with the Code in some areas. Under option 3, the draft code of practice would be implemented with no further draft regulations set out in secondary legislation. This option could change the way in which the Code or Practice is implemented and we are seeking further input on this in the survey we are running alongside this consultation.

6.101. We also note that, at the time we carried out the survey, the draft code of practice had not been published and respondents were asked to use a proxy for a future Code. Our updated survey will therefore also consider the impact of the published Code on these responses.

Direct Impact of Implementation Timetables

6.102. Whilst option 4 proposes different implementation timetables for Tier 1 providers and Tier 2 providers, option 5 proposes a consistent set of implementation timetables for both Tier 1 and Tier 2 providers.

6.103. It is worth noting that the implementation timeframes will be set out in the Code of Practice and not in the draft regulations. The timelines contained within the draft Code of Practice will serve as guidance on when government expects providers to have met their legal obligations, and Ofcom will take account of the code when monitoring compliance with the new framework. Should these dates not be met and sufficient mitigations or explanations not be provided, Ofcom may then take enforcement action using its new powers under the Telecommunications (Security) Act 2021.

6.104. For the smallest providers in Tier 3, we note that while Ofcom will focus on oversight of Tier 1 and Tier 2 providers, Tier 3 providers may choose to adopt the measures included within the draft Code of Practice where these are relevant to their networks and services.

6.105. Options 4 and 5 therefore have the potential to lead to different overall costs. First, this is because over the 10 year assessment period the costs of option 4 will be lower if Tier 2 providers begin complying with the draft regulations later. Our central estimate gives a total cost incurred by Tier 1 and 2 providers of £3.5bn over the next ten years in net present value terms. This is based on Tier 1 providers incurring one off costs over the years 2022 to 2026 and ongoing costs from March 2023 onwards. We assume that Tier 2 providers spread one off costs over an additional two years (six in total) and incur one off costs from March 2025. If Tier 2 providers began incurring both implementation and ongoing at the same time as Tier 1our central estimate would increase to £3.6bn.

6.106. Second, costs may differ if the implementation timetable guidelines impact costs for providers. There are a number of potential areas of incremental costs for smaller providers under option 5, as faster implementation might:

- reduce synergies with existing change programmes requiring providers to implement bespoke change programmes; or
- require external resources to manage change, requiring providers to pay more for personnel.

6.107. Whilst, these impacts might affect any provider they may affect smaller providers proportionately more if they have less capacity for organisational change.

6.108. Our updated cost survey will consider the extent to which option 5 will lead to higher costs and the reasons for this; including impact of implementation timetables on costs. We have opted to provide a quantitative assessment of option 5, after reissuing our cost survey, for the final impact assessment. The data gathered will help us provide a robust quantification of the costs to Tier 2 providers under this option.

Impact of Implementation Timetables on legacy equipment

6.109. Public telecommunications networks have evolved over many decades. While the UK is now transitioning to a gigabit-connected future, many network providers incorporate older, less functional technologies into the infrastructure that powers their services.

6.110. In some cases, plans are in place for phasing out legacy equipment and systems. For example, the copper-based analogue public switched telephone network (PSTN) is to be phased out by 2025. In December 2021, the Government and mobile network operators announced that mobile networks would move away from 2G and 3G by 2033 at the latest, with most expected to move earlier. In other cases, such as the move away from microwave links, discussions regarding impact and timing are ongoing.

6.111. The implementation timetables set out in options 4 and 5 seek to take into account existing public commitments to phasing out legacy systems. This includes the alignment

of significant technical changes that would affect fixed networks with the 2025 switch-off date for PSTN and transition to Voice-over-IP (VoIP) networks.

6.112. Where replacement timing is likely to be after the implementation of the framework (and so the requirements will need to apply to legacy equipment) the draft regulations and draft code of practice seek to address the impact of legacy equipment by:

- For support contracts which do not meet the minimum requirements the draft code of practice proposes measures that would record and mitigate the risks to networks and services.
- Measures recommending restricting unencrypted traffic to legacy systems in order to prioritise efforts on securing newer and more advanced networks.
- Setting out the need to protect systems that manage network administration by applying 'zones' for different activities. The effect will be to ensure that the most sensitive aspects of network management are not conducted over legacy systems.

6.113. Despite these mitigations some providers will incur costs securing equipment and systems considered 'legacy'. The consultation seeks to understand further the cost impact on equipment and systems considered 'legacy' as well as whether proposals in the draft regulations and draft code of practice address risks arising from legacy systems and equipment.

6.114. In addition, our updated cost survey will consider the extent to which option 5 will lead to higher costs and the reasons for this; including impact on legacy equipment.

Compliance and reporting costs incurred by industry

6.115. The Act gives Ofcom a new general duty to seek to ensure that public telecoms providers comply with their telecoms security duties. This gives Ofcom a clear remit to work with the telecoms providers to improve their security and monitor their compliance.

6.116. To allow Ofcom to fulfil this role, the Act provides Ofcom with powers to monitor and enforce industry compliance with the duties and requirements. It places expanded obligations on public telecoms providers to share information with Ofcom that is necessary to assess the security of their networks. Ofcom will also have the power to require public telecoms providers to complete system tests, to make staff available for interview and to allow authorised persons to enter providers' premises to, amongst other things, view equipment and observe tests. Ofcom will take any relevant provision of the codes of practice into account when carrying out its role.

6.117. In cases of non-compliance, Ofcom will be able to issue a notification of contravention to public telecoms providers setting out the suspected non-compliance, which should include details of any financial penalty Ofcom is minded to impose, and any remedial action Ofcom thinks should be taken. Ofcom is then able to confirm the imposition of said financial penalty or remedial action through a confirmation decision, should it consider it appropriate to do so. The Act also provides Ofcom with a new power to direct public telecoms providers to take interim steps to address security gaps during the enforcement process.

6.118. Ofcom is required to prepare and publish a statement of their general policy with respect to exercise of their functions by virtue of section 105Y of the Act. This statement will contain Ofcom's final reporting framework and is due to be published in advance of

commencement of the new framework in October 2022. The costs to industry of this framework will depend on the frequency and style of compliance reporting required.

6.119. For the purpose of this impact assessment, we have made the assumption that the reporting framework set out by Ofcom will require providers in Tiers 1 and 2 to produce annual reporting against compliance with the legislation. Ofcom may also issue assessment notices to providers which are likely to be information gathering exercises. These costs will be incurred directly by telecoms providers.

6.120. Deloitte produced a report in 2006 on the regulatory costs incurred by financial services firms in complying with specific FCA regulations[51]. The report considers incremental regulatory costs (costs that would not be incurred if the regulation did not exist) as a % of the total operating cost of each firm. In general, none of the requirements related to periodic reporting attracted high incremental regulatory costs. Although some of these activities are considered to be highly incremental in nature (i.e. the activities would largely not be undertaken in the absence of the FSA requirement), they are not in themselves high cost activities.

6.121. More specifically, the findings show that preparing and submitting quarterly/ monthly and annual financial return and annual accounts to FSA makes up 0.03% of total annual operating costs on average. Cooperating with FSA information gathering exercises makes up 0.02% of total costs on average. Similarly, submission of forms to vary permissions and modify rules makes up 0.02% on average. Finally, we have also included the costs of monitoring and maintaining externally generated financial resources in excess of requirement, which contributes 0.03% for total costs.

6.122. The total for all reporting costs is equal to 0.1% of total annual operating costs. We have used this as the central estimate for the percentage of total operating costs that Tier 1 and 2 providers will incur in meeting their reporting requirements under the new framework.

6.123. Due to the large variation of operating costs across Tier 1 and Tier 2 providers, a median annual operating cost figure of £285m has been used[52].

6.124. Based on this, compliance and regulatory costs will be £285,000 per year for Tier 1 and 2 providers. This value is based on the methodology used in the Deloitte report (2006), however a clarification interview with a Tier 1 provider suggests that this cost could be as low as £100,000 per year.

6.125. The total estimated annual cost of reporting is £11.4m for Tier 1 and Tier 2 providers. We have been unable to estimate split reporting costs for Tier 1 and Tier 2 providers. As a result, we have had to make a simplifying assumption that compliance costs are the same across Tier 1 and Tier 2 providers.

6.126. The draft code of practice, as set out in the consultation, proposes a three-phased approach to implementation. This is due to the variation in complexity and cost of the guidance as well as the different points providers will be starting from in regards to implementing the changes. Under this approach, Tier 2 providers will be given an additional two years to comply with each of the dates stated below. Tier 2 compliance dates are stated in brackets:

- **31 March 2023 (2025)** - proposed completion of the most straightforward actions achievable with minimal resource allocations

[51] The cost of regulation study, Deloitte, June 2006

[52] The annual operating cost of £285m is the median operating cost across Tier 1 and Tier 2 providers. The figure was sourced from the FAME company database.

- **31 March 2025 (2027)** - proposed completion of actions which require devotion of new resources and a degree of complexity
- **31 March 2026 (2028)** - proposed completion of actions that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions

Monitoring costs

6.127. Monitoring costs are costs incurred by Ofcom and DCMS in relation to the duties and powers set out in the Telecommunications (Security) Act. These costs are incurred directly by government (DCMS costs) and funded by government[53] (Ofcom costs). As a result we do not include these costs as a direct cost to business because the impacts do not fall on those businesses subject to the Regulation and accountable for compliance.

6.128. Those costs that Ofcom will recover directly from business - i.e. any costs relating to assessment and inspection notices - are discussed separately in the section on Compliance and reporting costs incurred by industry.

6.129. Ofcom already has responsibility for oversight of provisions of the CA which require network providers and service providers to ensure security and integrity of public electronic networks and services. As part of this responsibility Ofcom has published guidance, most recently updated in 2017[54].

6.130. Ofcom's role also includes following up and investigating reported incidents and any other concerns as needed and publishing a summary of incidents.

6.131. As a result of the Telecommunications (Security) Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, taking regard to the draft code of practice in their regulatory work.

6.132. The Department for Digital, Culture, Media & Sport (DCMS) will also incur additional costs in providing administrative support for the SoS under the new security regime.

6.133. It is expected that both Ofcom and DCMS will incur costs in carrying out these functions for the new security framework. We estimate these costs in Table 8 below based on information provided by both Ofcom and DCMS in April 2021.

6.134. Both Ofcom and DCMS estimates are based on a best guess of the future requirements for compliance and as such are subject to some uncertainty; we have therefore indicated a range of costs for each.

6.135. The Ofcom estimates have been submitted by Ofcom as their best estimates for the staff and non-staff costs incurred in fulfilling their responsibilities relating to the new telecoms security framework. The low estimates given below are Ofcom's base case estimates, not adjusted for risk, whereas the high estimates have had optimism bias applied.[55] Ofcom cost estimates are unlikely to change significantly with the

[53] Ofcom will recover these costs through negotiations of a rise in its spending cap via retention of the Wireless Telegraphy Act licence fees that Ofcom collects on behalf of HM Treasury.

[54] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003 2017 Version.

[55] For ICT costs, 95% optimism bias has been applied; for resource costs, 30%; for recruitment and training costs, 15%; for capital costs, 15%; and for all other costs, 41% optimism bias has been applied. These loadings were chosen by Ofcom.

implementation of our preferred option 4 or option 5 (Implementation plus), with the latter option not granting a 2 year grace period for Tier 2 providers.

6.136. The year 1 costs have been agreed with HM Treasury but the final costs for future years are subject to continuing discussions with HM Treasury as Ofcom works towards approval of final required spend.

6.137. DCMS costs are a best estimate of future resource requirements so we have indicated a range of costs, using a 25% discount on the base estimates to find the low estimate and a 25% load to find the high estimate.

6.138. These costs relate to the draft regulations; other costs will be incurred with respect to the national security powers in relation to high risk vendors:

Table 8: Costs of monitoring compliance with Part 1 of the Telecommunications (Security) Bill

	Total costs in net present value terms over the period 2021 - 2030 (3.5% discount rate), £m	
	Low estimate	High estimate
Ofcom costs	52.5	70.0
DCMS costs	0.8	1.4
Total	53.3	70.6

Options analysis: Compliance, reporting and monitoring costs

6.139. The Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021)) sets out the monitoring and compliance arrangements for the telecoms security framework. It provides Ofcom with a general duty to ensure providers comply with their new security duties, responsibility for monitoring compliance and enforcement powers to take action where providers are not meeting their obligations. Ofcom will publish guidance to explain how it will carry out its new role.

6.140. The options we have set out only affect the draft regulations and draft code of practice that will be put in place using powers provided by the Telecommunications (Security) Act. They will not affect the monitoring regime which was set out in that Act and is now contained in sections 105M to 105Y of the Communications Act 2003 (together with existing provisions in the Communications Act). Therefore any impacts on compliance, reporting and monitoring would be likely to be indirect in the sense that they would result from the way in which telecommunications providers implement the draft regulations and the Code and any subsequent impacts on compliance, reporting and monitoring costs.

6.141. This options analysis considers the impact of Options 3, 4 and 5 on compliance, reporting and monitoring costs that will be incurred by firms implementing the new security framework. We consider two potential impacts on:

- implementation of the guidance actions contained in the Code of Practice; and
- implementation timetables.

6.142. In the case of ‘implementation of the guidance actions contained in the draft code of practice’ we are using the survey accompanying this consultation to understand whether

option 3 could change the way in which the Code or Practice is implemented. For example, if more departures from the draft code of practice occur under option 3 this could impact on compliance, reporting and monitoring costs.

6.143. In the case of 'implementation timetables' this may affect the year in which telecommunications providers begin incurring compliance and reporting costs as under option 4 Tier 2 providers will only be expected to have implemented the first phase of measures by March 2025. Our current estimates assume that Tier 1 and 2 providers begin incurring compliance and monitoring costs in the third year of assessment.

6.144. Bringing compliance and reporting costs forward by two years for Tier 2 telecommunications providers would reduce our estimate of total costs over the 10 year assessment period. This would mean that costs would be higher under option 5. Monitoring costs are unlikely to change significantly if the framework were to be implemented earlier for tier 2 providers.

Indirect costs: Impact on the supply chain

6.145. The main indirect costs of this legislation are those incurred by businesses in the telecoms equipment supply chain. Whilst suppliers are not in scope of the draft regulations and do not incur direct costs as a result of these measures they are likely to be indirectly affected. We can view these costs as a type of pass through as the requirements are placed on to providers but are passed on to suppliers through contractual or other means. Suppliers may incur costs directly but recover these costs through pricing changes.

6.146. We also note that the supply chain for telecommunications equipment is a global market. A number of respondents including suppliers interviewed mentioned that the draft regulations could create incremental costs of operating in the UK. However, it is also the case that global equipment suppliers are likely to have the scale to absorb a degree of costs where they have a significant global security spend.

6.147. We have estimated the direct costs to PECN and PECS of each section of the draft regulations including section 7 on the supply chain. We do not separately estimate the costs to suppliers of these requirements. However, we consider the evidence available on the number of suppliers and the impact on suppliers below.

6.148. We estimate that there were at least[56] 104[57] suppliers in the UK's telecommunications sector from 2017 to 2021, based on publicly announced carrier-vendor contracts. This is in contrast to 746 suppliers who operated globally over the same time period.

6.149. Our survey of PECN and PECS included questions on the potential impact on suppliers - although these were only asked to larger respondents. Respondents were asked to indicate - on a scale - what proportion of their suppliers would be affected by the draft regulations. The most common response was:

- That all or some of their network equipment suppliers will be affected; and
- That some third party administrators will be affected.

[56] This estimate of the number of vendors in the UK is a conservative lower bound, with the actual number potentially higher at a few hundred.

[57] Omdia holds a database of publicly announced contracts between communications providers and vendors globally between 2000-2020 in the wireless and fixed access markets. We have used data on UK-based contracts as of Q2 2020.

6.150. In addition, respondents were asked whether they thought the draft regulations would affect the number of suppliers participating in procurements; 70% of respondents thought that the number would reduce.

6.151. We also carried out a small number of bilateral interviews with suppliers to validate these findings. The suppliers we spoke with indicated that they expected to be affected by the requirements but were unable to indicate the scale of the impact at this stage. This is consistent with the stage of implementation of the draft regulations - the impact on suppliers will be driven by the implementation of the draft regulations by providers.

6.152. The most common cost drivers noted for suppliers as a result of the proposed draft regulations, were highlighted as but not limited to; legal and contractual amendments, patching, audit, recruitment of new personnel, monitoring and testing. It was also noted that the costs were likely to be one off in nature. Concerns have also been raised that the new draft regulations will disproportionately affect smaller vendors' ability to supply providers - this is in line with our survey responses which indicated a potential impact on the number of suppliers participating in procurements.

6.153. In summary, there is some evidence that suppliers will incur indirect costs as a result of pass through of requirements by PECN and PECS. However, the level of costs is highly uncertain. The degree to which these costs will be passed through to PECN and PECS is not known but we note that many suppliers will be able to spread these costs over a number of supply contracts.

Indirect costs: impact on consumers

6.154. We also consider that end users of telecoms networks and services may potentially incur costs as a result of telecoms providers passing the costs of compliance onto consumers. The extent to which changes in network costs are passed through to consumers depends on the level of cost reduction as a proportion of total cost and the rate of cost pass-through. A 2009 report by the International Telecommunications Union (ITU) found that the pass-through rate of costs to consumer prices was 69% in the mobile telecoms market and 26% in the fixed telecoms market.[58] Costs that are not passed through to consumers are either retained by telecommunications providers or are passed through to network investment expenditure. This means that in addition to the pass-through of costs to consumers, costs incurred by telecoms providers could also lead to less investment in networks.

6.155. Our analysis shows that the new security framework will lead to material costs for telecommunications providers in the UK. Since we have only quantified the total costs incurred by telecom providers in this impact assessment, and not the total benefits, we do not have an estimate for the total net costs incurred by telecoms providers. Based on our benefits analysis, detailed in the next section, we assume that the total net costs to business will be low and so the pass-through cost to consumers will be minimal.

Economic Impact - benefits

6.156. This section details the potential economic benefits of improving the security and resilience of 5G and full fibre networks in the UK through the Telecommunications (Security) Act.

[58] Mobile Termination Rates: To Regulate or not To Regulate, ITU, 2009

6.157. The legislation will support the growth of 5G and full fibre networks in the UK by ensuring the security of these networks. As stated in the Supply Chain Review, the widespread deployment of 5G and full fibre networks is a primary objective of government policy. These networks will be the enabling infrastructure that drives future economic growth. The security of these networks is in the UK's economic interest. If these networks are judged to be insecure, their usage and economic value will be significantly reduced.

6.158. The new security framework will reduce our vulnerability to cyber risks. The potential costs of a security compromise are broad; the framework will help harden the network against such an incident, reduce security risks by reducing the impact of a cyber attack or network outage.

6.159. Table 9 sets out the potential benefits of the draft regulations identified by providers in our cost impact survey, which received 22 responses

Table 9: What benefits do you expect will accrue to your business from implementation of the draft security requirements to be contained in secondary legislation? All responses[59].

Answer	Percentage of respondents that selected this benefit
Detect security compromises earlier	19%
Improve ability to rectify security compromises	18%
Reduce severity of security compromises	13%
Reduce number of security compromises	12%
Improve offering to customers	8%

6.160. In this section we consider the impact of cyber attacks, breaches and unintentional incidents; many of which have detrimental impacts, often in the form of network disruption or data loss.

6.161. We also consider the economic benefit arising from 5G use cases, where network security and resilience are considered a prerequisite to their adoption. These are a key indirect[60] benefit resulting from the new security framework.

6.162. We have not included these benefits in the impact assessment calculator. This is because doing so would require us to make an assumption about what proportion of benefits to attribute to the new security framework - we do not have any information on which to base such an assumption.

[59] Note: Top five responses. Respondents were asked to tick all that apply.

[60] An indirect effect can be described as a general equilibrium effect occurring in related markets and/or the wider economy, coming from first round effects in the regulated market that are sufficiently large to result in changes in other markets In this instance the first round effect is in the downstream telecommunications market which can affect other markets such as those sectors that are expected to utilise telecommunications technology to create wider economic benefits. See RPC case histories, Direct and Indirect Impacts, March 2019.

Evidence of current vulnerabilities in the network

6.163. As wider UK Critical National Infrastructure becomes more dependent on the UK's telecoms networks with the roll-out of full-fibre and 5G, it is vital that security concerns are properly accounted for and addressed.

6.164. There is clear evidence of the telecoms sector's increasing vulnerability to security incidents prior to the pandemic.

6.165. Nexguard's DDoS Threat Report, which is a quarterly report measuring thousands of distributed denial-of-service (DDoS) attacks around the world, found that nearly two thirds of DDoS attacks in the third quarter of 2018 targeted communications service providers[61]. EfficientIP's 2017 Global DNS Threat Survey Report, which surveyed 1,000 global telecoms providers and vendors, states that 25% admitted they have lost sensitive customer information as a result of a DNS attack[62]. This is higher than any other sector surveyed.

6.166. As well as security attacks, telecoms networks are vulnerable to outages which have an impact on all users of networks. In 2019, of the 61 serious or severe outages that made headlines globally, 30% were caused by network issues, according to a 2020 Uptime Institute Report[63]. This was the second biggest cause of outages, narrowly surpassed by IT system issues at 31%.

6.167. In January 2020, the NCSC published a report that gave two recent examples of security incidents occurring in the UK relating to the signalling plane and supply chain:

- Within the last five years, a major telecoms network was accidentally remotely disabled for a number of hours due to the failure of a critical core node to process an unusual, internationally-routed signalling message. While this failure was an accident, it highlights a potential vulnerability that could be intentionally abused unless mitigated. Furthermore, signalling networks have been shown to allow the leaking of subscriber and network data, sometimes in support of criminal activity.
- On 20 December 2018, HMG attributed a cyber attack targeting several global managed service providers (MSPs) to China-linked group APT10. Through compromise of these MSPs, APT10 had managed to exploit multiple customers of those MSPs and exfiltrate a high volume of data. The overall scale of the compromise was unprecedented, and had gone undetected since at least 2016.

Other recent case studies of security incidents in the UK include the below:

- O2 suffered a major network failure in December 2018 due to an expired certificate in Ericsson software, which resulted in a loss of data services. 32.1m users in the UK had their data network go down for up to 21 hours. Other services which rely on O2's network, such as TfL's live bus timetable and all the apps that make calls to the API also went down.[64]
- Hackers targeted TalkTalk in October 2015 stealing around 1.2 million customers' email addresses, names and phone numbers, including 157,000 dates of birth and 16,000 bank account numbers and sort codes.[65]

---

[61] https://www.nexusguard.com/threat-report-q3-2018, 2018

[62] https://www.efficientip.com/dns-security-telecom-sector/, 2017

[63] Uptime institute: Annual outage analysis, 2020

[64] Why millions of Brits' mobile phones were knackered on Thursday: An expired Ericsson software certificate, The Register, December 2018

[65] https://www.telegraph.co.uk/news/2018/11/19/talktalk-hackers-jailed-18-months-2015-cyber-attack-caused-misery/

- In March 2015, internet traffic for 167 BT customers, including a UK defense contractor that helps to deliver the country's nuclear warhead program, was illegally diverted to servers in Ukraine before being passed along to its final destinations.[66]
- According to the NCSC, one company affected by the so-called NotPetya attack in June 2017 had to install 4,000 new servers, 45,000 new PCs and 2,500 new applications.[67]
- In 2016, UK mobile provider Three was hacked, resulting in the theft of personal data from 134,000 customers. The hackers accessed information using employee login details.[68]
- In 2016 it was reported that malicious software known as the 'Mirai Worm' had infected around 100,000 Post Office routers in the UK. The hacked routers were used to route internet traffic to popular websites including Netflix and Twitter.[69] An independent testing body suggested that this could have arisen from a weakness in some of the routers' software.[70]

6.168. The reliance of the country on telecoms networks has only increased in the face of the COVID-19 pandemic. After triggering an unexpected, accelerated shift to digital technologies and services, the pandemic placed immense pressure at the feet of the UK telecoms industry. This shift has further highlighted the importance to address security incidents in the sector.

6.169. According to a 2020 study by IBM, a majority of organisations (54%) required remote work at the height of the COVID-19 pandemic[71]. This is compared to 5% of workers working from home all the time in January to March 2020, according to a survey undertaken by the Chartered Institute of Personnel and Development (CIPD)[72].

6.170. This trend in remote working makes it more vital than ever to ensure households and businesses are kept online with as few disruptions as possible.

6.171. Evidence suggests that the frequency, severity and costs of cyber attacks on the telecoms industry is worse than the average UK sector. This is supported by evidence from the recent Cyber Security Breaches Survey, undertaken by Ipsos Mori and published by DCMS in March 2020[73]. The information and communications sector has, across each year of the survey, consistently stood out as more likely to identify breaches. 62% of information and communications companies have identified breaches or attacks in the last 12 months, compared to 46% across all UK sectors and 47% for the same sector last year.

6.172. A report from OGL Computers found that 75% of SME IT and telecoms companies in the UK suffered 2 or more cyber attacks in 2020[74].

---

[66] https://arstechnica.com/information-technology/2015/03/mysterious-snafu-hijacks-uk-nukes-makers-traffic-through-ukraine/

[67] Ciaran Martin's speech at the CBI Cyber Conference, 12 September 2018

[68] Three Mobile hack affected 76,000 more customers than thought, The Telegraph, March 2017

[69] The Mirai Botnet Isn't Easy to Defeat | WIRED, Wired article, December 2016

[70] TalkTalk router hack. Consumers, what should you do? Pen Test Partners blog post, security consultants

[71] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

[72] Flexible working arrangements and the impact of the COVID-19 pandemic | CIPD

[73] Cyber Security Breaches Survey 2020: Statistical Release, 2020. The survey is an official statistic and constituted a random probability telephone survey of 1,348 UK businesses and 337 UK registered charities from 9 October 2019 to 23 December 2019.

[74] OGL, State of Technology Research Report

6.173. The proposals set out in the preferred option seek to address these vulnerabilities and protect UK security and prosperity.

Costs of security incidents

6.174. In terms of costs, there is a range across the literature and case studies, however, there is a general pattern of these costs being significant.

6.175. The Cyber Breaches Survey states that the average cost of all the cyber security breaches experienced in all sectors in the past 12 months is estimated to be £3,230. For medium and large firms, this average cost is higher at £5,220. The findings of the Cyber Breaches Survey have been extrapolated to provide a cost estimate across all UK businesses. The estimated cost to UK businesses of cyber breaches is £648 million in the central scenario, within a range of £356 million to £939 million (with a 95% confidence interval). It is important to note that survey respondents were asked to self-report their costs[75]. Additional DCMS research[76] has shown that respondents do not fully count all economic costs, instead focusing on direct financial impacts. As such, the figures are more often than not an underestimate.

6.176. The IBM 2020 Cost of Data Breach Report found that the average total cost for UK data breaches between August 2019 and April 2020 was $3.90 million.[77]

6.177. An EfficientIP report found that, specifically for the telecoms sector, the average cost of a single cyber attack was $600,000 in 2017 (global figure)[78]. Furthermore, 5% of telecoms organisations surveyed stated an attack cost them more than £3.75 million.

6.178. According to a recent Accenture report, the average annual cost of cybercrime for a company with over 5,000 employees was $11.5m in 2017[79].

6.179. Of the case studies discussed above, only the TalkTalk and NetPetya incidents have associated costs publicly available. The total cost to TalkTalk was £60m and the cost to the company affected by the NetPetya attack was estimated at £150 to £250 million[80].

6.180. In many cases, a security compromise also has a reputational impact on the affected company. According to a CGI and Oxford Economics report, an organisation's share price falls by an average of 1.8% following a severe breach. This is equivalent to a £120m loss of FTSE 100 company value following a severe cyber breach. In extreme cases, cyber breaches have reduced a company's share price by 15%[81].

---

[75] Survey respondents were asked to consider costs arising from new measures needed for future attacks, added staff time to deal with breach or inform others, stopped staff carrying out daily work, loss of revenue or share value, prevented provision of goods and services, complaints from customers, reputational damage, goodwill compensation to customers, fines or legal costs and other repair or recovery costs

[76] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf

[77] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf For the 2020 Cost of Data Breach Report*, Ponemon Institute recruited 524 organizations that experienced data breaches between August 2019 and April 2020. The organizations in the study are of various sizes, spanning 17 countries and regions as well as 17 industries.

[78] EfficientIP, DNS Security: The Telecom Sector's Weakness, 2017

[79] Accenture, THE COST OF CYBERCRIME 2019. Statistic based on a sample of companies with 5,000 plus enterprise seats

[80] Ciaran Martin's speech at the CBI Cyber Conference, 12 September 2018

[81] CGI, The Cyber-Value Connection, 2018.

6.181. All of the estimates given here suggest that the cost of a security breach or attack for a UK telecoms company could be anywhere in the range of £3,000 to £250m. For the purpose of the impact assessment, we have made some key assumptions to provide an illustration of the potential benefits associated with the improved security of telecoms networks. We have used the EfficientIP and Accenture cost figures, as well as the CGI share price impacts, to estimate the total cost of security compromises affecting providers of PECN and PECS in the UK over the next ten years.

6.182. We have assumed that for Tier 1 and 2 providers, the current annual cost of cyber security compromises is equivalent to £8.2m per company, as set out in the Accenture report. We have also assumed that, over the next ten years, there will be two severe incidents which reduce the share price of the affected provider, resulting in a loss of £120m per incident. This is based on the occurrence of two severe cyber compromises affecting major telecoms companies in the UK in the years 2011-20[82].

6.183. We have assumed that 75% of Tier 3 providers currently suffer at least 2 security compromises each year, based on the OGL report. We have used an average cost per breach of £426,000, based on the EfficientIP report, to estimate the current annual cost of compromises for Tier 3 providers.

6.184. Table 10 shows the total cost of security compromises for PECN and PECS providers over the years 2024 - 2031. This period starts in 2024, the year after the first phase of measures in the code of practice are expected to be implemented, giving time for them to begin to impact on the costs of security compromises. This will continue to the end of the impact assessment period.

Table 10: Monetisable costs of security compromises for PECN and PECS providers, discounted at 3.5% over 2024-31

	Total cost (£bn)
Tier 1 providers	0.43
Tier 2 providers	1.74
Tier 3 providers	1.75
Share price impact	0.20

6.185. The total cost over the years 2024-2031 impact assessment period of security compromises for PECN and PECS providers is estimated to be **£4.1bn**. Considering a shorter period (2026-2031) for Tier 2 and 3 providers reflecting later implementation of the draft regulations would reduce the costs to **£3.2bn**.

6.186. We have conducted some sensitivity analysis on these assumptions. In the low cost scenario, we assume that Tier 2 providers incur the same annual costs as Tier 3 providers and that there will only be one severe security compromise impacting the share price of a Tier 1 provider. In this case, the total cost of security compromises over the period is **£2.4bn**. In the high cost scenario, we assume that all Tier 3 providers suffer at least one security compromise annually and that there will be three severe security compromises impacting the share price of a Tier 1 provider. In this case, the

[82] The O2 failure in 2018 affected 32.1 million customers; the TalkTalk hack in 2015 affected 1.2 million customers.

total cost of security compromises over the period is **£4.5bn**.

6.187. The new security framework introduced by the Act will reduce the cost impact of security compromises in two ways. Firstly, any security compromises that do occur are likely to be identified and dealt with at an earlier stage due to the monitoring and analysis requirements in the draft regulations. Providers are required to monitor incoming and outgoing communications to identify and investigate anomalous activity. The remediation and recovery requirements in the draft regulations are aimed at making sure networks can be recovered after any security compromises. In the UK, it takes an average of 181 days to identify a data breach and 75 days to contain it[83]. The average cost savings of containing a breach in less than 200 days, compared to more than 200 days is $1.12 million[84], representing a 26% reduction in the average cost of a breach.

6.188. Secondly, the security improvements that will result from the draft regulations could lead to a reduction in the number of security compromises. The new security framework set out in the draft regulations will help to harden the network against such an incident and reduce the likelihood of occurrence. Examples of the requirements that directly protect the network from security compromises include:

- Regulation 3 - Network architecture: This includes keeping the most sensitive parts of their network separate to the less sensitive parts.
- Regulation 7 - Prevention of security compromise and management of security permission: This Regulation contains measures to protect networks by controlling who has permission to access network functions. This includes using best practice technical solutions like multi-factor authentication and limiting the number of people given security permissions. It also requires providers to be able to isolate the parts of the network which are essential for it to run from any unsafe signals that come from outside the network.
- Regulation 9 - Governance and accountability: amongst other things, providers must also identify and prioritise necessary network security updates and network equipment upgrades.
- Regulation 11 - Testing: This Regulation ensures that providers must carry out or arrange tests on their network or service to assess the resilience of the network or service to security risks. These tests should simulate, as far as is possible, active techniques and realistic situations that might be expected to be used by an attacker.

6.189. The new security framework will reduce the cost impact of security compromises reducing the total cost of security compromises. However, we have not estimated the proportion of costs that would be avoided.

Benefits to consumers of improved telecommunications security

6.190. In the above section, we have monetised the potential benefits to telecoms providers of improved security. Improved security will also benefit consumers, specifically, the customers of telecoms providers. There were 83.8 million active mobile subscriptions and 27.5m fixed broadband connections in the UK by the end of 2020[85]. A reduction in the frequency and severity of security compromises in telecoms networks and services

[83] IBM, Cost of a Data Breach Report 2020

[84] ibid.

[85] Telecoms Data Update: Q4 2020 (ofcom.org.uk)

will impact consumers in a number of ways. For example, reductions in network outages will enable more continuous access to phone and internet services for consumers. The O2 outage in 2018 took 32.1 million customers offline, interrupting both business and personal activities being undertaken over their mobile data network. Studies have shown that consumers value network access and resilience. A study by Rand Europe (2014)[86], for example, found that residents in UK not-spot areas are willing to pay up to £23 more a month for better quality service.[87] A study by Lee and Cho (2018)[88] found a mean monthly willingness-to-pay to avoid communication failure of USD 0.80 per user in South Korea.

6.191. Another example is data loss: in 2015, a cyber attack on TalkTalk resulted in the loss of personal details for 1.2 million customers. A reduction in the frequency and severity of cyber attacks on telecoms providers will help to ensure that personal customer data held by providers remains secure and uncompromised.

6.192. We have not monetised the benefits to these customers to avoid double counting. We have already monetised the costs to telecoms providers of cyber security incidents, and we consider that these cost figures may include compensation to customers. However, it is clear that the improved security of telecoms networks and services due to the new security framework will benefit those that use them.

Economic benefits of 5G and Full Fibre

6.193. The uptake and adoption of 5G and full fibre networks in the UK is strongly dependent on a dependable level of security and resilience within these networks. The Review states that 'the potential economic and social benefits of 5G and full fibre digital connectivity can only be realised if we have confidence in the security and resilience of the underpinning infrastructure. The widespread deployment of 5G and full fibre networks is a primary objective of government policy. These networks will be the enabling infrastructure that drives future economic growth. The security of these networks is in the UK's economic interest. We define security as safeguarding the availability, integrity and confidentiality of the UK's telecoms networks. If these networks are judged to be insecure, their usage and economic value will be significantly reduced.'[89]

6.194. These communications services have never been more important than in the last year. The Covid-19 pandemic has highlighted the importance of connectivity for UK consumers as a vital part of how businesses and people communicate and consume information and entertainment. The steps taken by the UK and devolved governments in response to Covid-19 meant that, during 2020, people relied even more than before on fast, reliable broadband connections in their homes. The UK's fixed access networks have seen significantly increased demand from users in 2020, and compared to periods before the lockdown, mobile voice traffic increased by 10-45% across the providers[90].

---

[86] Rand Europe (2014). Estimating the value of mobile telephony in mobile network not-spots.

[87] Better quality service in the paper's context is defined as levels that are of higher quality relative to those in areas adjacent to the not-spots.

[88] Lee & Cho (2018). Inconvenience cost of mobile communication failure: The case of South Korea.

[89] UK Telecoms Supply Chain Review Report, 2019

[90] Connected Nations report 2020, Ofcom

6.195. This dependence on secure and reliable telecommunications networks is expected to continue into the future. A survey of just under 1,000 firms conducted in September 2020 by the Institute of Directors (IoD) shows that 74% plan on maintaining the increase in home working[91].

6.196. Several recent reports have estimated the economic benefits of 5G and full fibre-to-the-premises broadband (FTTP) networks to the UK. However, the Covid-19 pandemic and the high risk vendor (HRV) decision made by government in July 2020[92] have impacted the speed at which these networks will rollout. We have considered these impacts in more detail in the next section.

6.197. An independent report from the Centre of Policy Studies finds that, despite the impact of the Covid-19 pandemic, a potential £34.1bn of additional economic output could be created if the government delivers its 5G target of covering the majority of the population by 2027, and more than £40bn if it is exceeded[93].

6.198. As for full fibre, a report from the Centre of Economics & Business Research estimates a gross value added (GVA) uplift of £59 billion by 2025 if deployment is completed at that point – with benefits continuing to rise after deployment is complete. The report forecasts and additional £16.1bn on GVA due to workforce impacts of network deployment[94]. Even with the impacts of Covid-19 and the HRV decision, the government stated in November 2020 that it aims with industry to deliver a "minimum of 85%" gigabit-capable coverage by 2025[95].

6.199. These reports give an illustration of the scale of 5G and full fibre networks in the UK, to provide context around the market impacted by this legislation.

6.200. The following analysis makes the argument that the economic value generated by a number of 5G use cases are dependent on secure and resilient networks. Without this legislation, the full extent of these benefits will not be realised.

The new security framework will unlock 5G use cases that would not have been deployed under a lower level of security

6.201. From our literature review of twelve reports[96] published over the last 5 years that have estimated the economic impact of 5G, it is clear that the value of 5G is derived from the potential use cases for businesses and governments. Some examples of these use cases include: smart LED street lighting, which can be dimmed or brightened remotely as needed; 5G sensors on railway lines to improve predictive maintenance; and remote monitoring of soil temperature and moisture, crop development and livestock on farms.

6.202. The existence of 5G networks is a prerequisite for realising the full potential of these use cases. This is widely supported within the relevant literature, summarised in the following statement from Cambridge Wireless:

> '5G telecommunications promises not just high bandwidth, but also low latency (increased responsiveness) and an ability to encompass The Cloud and a host

[91] Home-working here to stay, new IoD figures suggest | Institute of Directors | IoD, September 2020
[92] Huawei to be removed from UK 5G networks by 2027, Gov.uk, 14 July 2020
[93] Upwardly Mobile: How the UK can gain the full benefits of the 5G revolution, October 2020
[94] Full fibre broadband: A platform for growth, October 2019
[95] National Infrastructure Strategy - GOV.UK, November 2020
[96] Research into the economic benefits if 5G is relatively limited so we have taken the twelve reports that we consider to have a robust methodology.

of devices attached to the network. As a result, the linkage of connected devices through the Internet of Things (IoT) will create increasingly complex networks, while other systems that require massive amounts of data transfer such as autonomous vehicles, robotic surgery, and critical infrastructure monitoring will see big gains in efficiency.'[97]

6.203. The literature shows that some of the use cases rely heavily on networks that are highly secure and reliable. This is backed up by the finding in a 2018 Ericsson report[98] that the two main barriers to 5G adoption are concerns around data security and privacy and lack of standards.

6.204. The new security framework will help harden the network against attack and reduce security risks by reducing the impact of a cyber attack or network outage. Therefore, we are making the assumption that the new security framework will contribute to unlocking those 5G use cases that are particularly dependent on secure and reliable networks. The improved level of security in the network will encourage the rollout and take up of these use cases where they would not have been deployed otherwise.

6.205. Therefore the quantifiable benefits of the new security framework are the benefits of the 5G use cases that are particularly dependent on secure and reliable networks. In order to quantify these, we have looked at the economic benefit of 3 use cases highlighted by the Ericsson report as having a particular reliance on secure and reliable 5G networks:

- Remote medical examination
- Remote health monitoring
- Autonomous cars

6.206. We have estimated the economic value of these cases based on findings in the literature. Table 11 below shows the estimated benefits in the central scenario.

Table 11: Monetisable benefits of each 5G use case, discounted at 3.5% over 2022-30

Use case	Economic benefit (£bn)
Remote medical examination	6.8
Remote health monitoring	7.4
Autonomous cars	12.5
Total (2022-31)	26.8

6.207. The total monetisable benefits of the three identified use cases over the impact assessment period of 2022 and 2031 is estimated to be £26.8bn, in present value terms. However, we note that these benefits are dependent on the roll out of 5G networks and do not begin to accrue until 2026 or 2028 in the case of autonomous cars. The analysis that makes up this figure is detailed in Annex 1.

6.208. We have conducted some sensitivity analysis on these wider benefits to illustrate the impact of varying our assumptions. As a base case, we mapped the estimated benefits to the UK found in the literature for each use case across the ten year impact assessment period. In the central scenario, shown in Table 4, we have delayed the accrual of benefits by 3 years to reflect the delay in 5G rollout assumed to result from

[97] How 5G Could Transform the Delivery of Healthcare

[98] Ericsson report - Industry Impact of 5G 2018.pdf

any potential decision to use the HRV powers in the Act [99]. This includes a one year delay as a result of the Covid-19 pandemic, as estimated by a 2020 PwC report[100].

6.209. In the optimistic scenario, we assume that the use of any the HRV powers in the Act would not delay rollout significantly. In this case, we have assumed a one year delay coming from Covid-19 only. In this case, the total monetisable benefit, discounted at 3.5% over the next 10 years, increases to £45.3bn.

6.210. In the worst case scenario, we have assumed a 3 year delay resulting from the HRV decision and Covid impacts, as well as a further two year delay in the deployment of the individual use cases. 5G use cases are still in trial for the most part and we have applied this sensitivity analysis to account for the risks associated with the application of such a nascent technology. In this case, the total monetisable benefit, discounted at 3.5% over the next 10 years, falls to £13.0bn. A delay of two years reflects our estimate of the most likely worst case delay in deployment across the three use cases. Most of the sources we reviewed place the estimated deployment date within two years either side of the deployment date modelled in the original analysis.

6.211. Furthermore, not all of these benefits can be attributed to the new security framework. Improved security may be the most important enabler for the deployment of these use cases, but other factors such as innovation, skills and access to finance are also required. Improved security may also not be a requirement for 100% of the benefits and some could accrue regardless. Additionally, 5G may not be a requirement for all of the benefits; 4G may allow for some functionality such as non-urgent, routine medical examinations, but not to the extent that 5G allows.

6.212. Finally, we do not know the contribution of private networks to the deployment of these use cases. The legislation applies to public network and service providers only, and while the draft regulations will serve as best practice security guidance for all UK telecoms providers, private networks are not obliged to improve their security under this framework.

[99] Huawei to be removed from UK 5G networks by 2027, Gov.uk, 14 July 2020

[100] Countering the Threat to Europe's 5G Rollout | Strategy& Europe, PwC, 2020

Costs and benefits to business calculations

6.213. We have estimated three types of direct costs to business as a result of the draft regulations. These are: familiarisation costs; implementation and ongoing costs; and compliance and reporting costs. We have also estimated the costs incurred by Ofcom and DCMS of monitoring and managing the new security frameworks.

6.214. The most significant cost type is implementation and ongoing costs; these are the costs to business of meeting the draft regulations. We estimate these costs for larger providers in scope of the new security framework and in Tier 1 and 2 of the draft code of practice. Our estimates fall in a wide range. In summary we found that over the impact assessment period, Tier 1 and 2 providers:

- could incur one-off costs in a range from £1,090m to £2,520m in present value terms assuming that these costs are incurred by all providers over the years 2022 - 2026. If smaller providers spread one-off costs over an additional two years later this would reduce to £1,080m to £2,510m in present value terms.
- could incur average annual ongoing costs in a range from £100m to £240m per year in present value terms assuming that these costs are incurred by all providers from March 2023 onwards. If smaller providers incur one-off costs two years later this would reduce to £95m to £230m per year in present value terms.

6.215. We estimate familiarisation and compliance and reporting costs for all providers. In total we estimate familiarisation costs will fall in a range from £3.7 - £4.9 million net present value over the impact assessment period; and compliance and reporting costs will be approximately £11.4 million annually.

6.216. On the other hand there are significant benefits of the new security framework and these benefits are both direct benefits to telecommunications providers and users and indirect benefits that benefit the wider economy. We have focused on two types of benefits where we are most able to estimate the economic impact. These are:

- the direct benefits of reducing the cost of potential security compromises
- the indirect benefits of unlocking 5G use cases

6.217. Whilst we have monetised these benefits, we have not included them in the final calculation of net impact or EANDCB as doing so would require us to make an assumption about what proportion of benefits to attribute to the draft regulations. We do not have sufficient information to make this assumption.

6.218. Instead, we have presented an illustrative breakeven analysis between the direct costs and the potential direct benefits for Tier 1 and Tier 2 providers in Table 12 to assess the magnitude of the policy. Due to the uncertainty in the original Tier 3 cost estimates and our intention to reissue a new cost survey alongside the public consultation, we have omitted these figures from our current breakeven analysis. We hope that further data from Tier 3 providers will allow us to estimate breakeven analysis for all Tiers.

6.219. Breakeven analysis is an analysis tool often used when the cost of an intervention is known and the value of the potential outcomes that are realised are also known; but there is no estimate of the impact of the intervention on the outcome. It calculates the proportion of the positive outcomes that need to be realised in order to cover the cost of the intervention. In this case, we compare the direct costs and benefits estimated in this section (the direct benefits are the reduction in costs of potential security compromises). We use this to calculate

the proportion of the benefits that would need to be attributable to improved security for those benefits to equate to the costs of the policy. We have shown the central scenario, best-case scenario and worst-case scenario for Direct benefits in Table 12.

Table 12: Direct costs and benefits net present value figures over period 2022-31, discounted at 3.5% (excluding one off and ongoing costs for Tier 3 providers)

	Direct costs*[101] (£m)	Direct benefits (£m)	% of total benefits that need to be realised to break even*
Central scenario	3,579	4,120.4	87%
Best-case scenario	2,104	4,499.6	47%
Worst-case scenario	4,920	2,412.4	204%

*Excluding one off and ongoing costs for Tier 3 providers.

6.220. This analysis shows that, in the central scenario, direct benefits are £4.1bn if they begin to accrue in 2024 although considering a shorter period (from 2026) for Tier 2 and 3 would reduce this to **£3.2bn**. Whilst we have not estimated the total costs to smaller providers, we estimate that costs to larger providers, familiarisation costs for all providers and costs incurred by government and Ofcom to be a present value of £3.6bn over 10 years. In the scenario whereby Tier 2 and Tier 3 benefits accrue later, the direct benefits, under the central scenario, will not compensate for the direct costs, however, the exclusion of Tier 3 costs mean such interpretations are illustrative at this stage.

6.221. However, it is important to note that our estimated benefits figure uses an average annual cost of cybercrime for enterprises with at least 5,000 enterprise seats[102] as a proxy for the costs of cybercrime to Tier 1 and 2 providers. However, a single incident can have a much more significant impact, for example, the total cost of the TalkTalk case study cited above was £60m and the cost to the company affected by the NetPetya attack was estimated at £150 to £250 million[103]. Furthermore, whilst CGI and Oxford Economics found that an organisation's share price falls by an average of 1.8% following a severe breach, in extreme cases, this impact has been as high as 15%[104].

6.222. As stated, we do not expect that all of these benefits will be realised as a result of the new security framework. These benefits represent the total costs of security compromises to telecoms providers as far as we have been able to monetise them. While we expect that the new framework will reduce the frequency of compromises to a certain extent, we also expect that compromises will still occur but may be identified

[101] These costs include only the direct costs included in the business impact calculator i.e. one-off and ongoing costs incurred by all Tier 1 and 2 providers and Tier 3 providers with code powers, and familiarisation and reporting costs incurred by all providers.

[102] Enterprise seats represent the number of people connected to networks or systems within an organisation.

[103] Ciaran Martin's speech at the CBI Cyber Conference, 12 September 2018

[104] CGI, The Cyber-Value Connection, 2018.

earlier due to the improving monitoring measures required by the framework. IBM found that identifying and containing a breach early reduces the cost by an average of 26%[105].

6.223. We have not included the wider benefits of 5G use cases that are reliant on highly secure and resilient networks in the above table. We note that the benefits of 5G use cases are indirect and would not be included in the net direct cost to business but in the wider net present social value. However, to demonstrate the scale of the wider benefits, we have set them out in table 13 below.

Table 13: Net present value figures for wider benefits over period 2022-31, discounted at 3.5%

£bn	Direct benefits (costs of security compromises)	Indirect benefits (5G use cases	Total
Central scenario	4.1	26.8	30.9
Best-case scenario	4.5	45.3	49.8
Worst-case scenario	2.4	13.0	15.4

6.224. As noted, only a small proportion of these benefits can be attributed to the new security framework. However, if just 5% of these benefits could be attributed to the impact of the new security framework that would create benefits of £1.3bn. Furthermore, these benefits are **focused on a small number of use cases, but there are also wider benefits associated with the rollout of full fibre and 5G networks. These wider benefits of the rollout of these networks may include additional use cases for which security and resilience are important which would indicate a set of much larger potential benefits.**

[105] IBM, Cost of a Data Breach Report 2020

7. Risks and assumptions

7.1. In carrying out this impact assessment we have assessed the direct costs to industry of implementing the draft regulations based on the early illustrative draft Electronic Communications (Security Measures) Regulations published on 13 January 2021. The draft regulations have been developed from detailed security analysis conducted by the NCSC that used a sophisticated threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[106]. An early draft of the regulations was published in January 2021 to gather industry feedback[107]. The draft regulations published for formal consultation alongside this assessment have been updated to account for that initial feedback. They aim to address the security risks facing public networks and services providers by providing appropriate and proportionate security requirements in law with which public telecoms providers must comply. Ofcom, as the independent telecoms regulator, will be responsible for monitoring and enforcing compliance with the statutory requirements.

7.2. In making this assessment we have made assumptions about the efficacy of the draft regulations and the accompanying draft code of practice including that PECN and PECS will comply with the draft regulations and implement the requirements in a way that meets the objectives of the security framework (the Act and the Regulations). In turn that this implementation will create security benefits and that these benefits will be maintained across the impact assessment period.

7.3. In the table below we set out key assumptions that relate to the risks to the policy objectives of this security framework. For each risk we set out the key assumption that we have made; any evidence collected that relates to that assumption; a description of the risk and any associated mitigations and a description of any sensitivity analysis undertaken:

[106] Summary of the NCSC's security analysis for the UK telecoms sector, January 2020

[107] Early illustrative draft of Electronic Communications (Security Measures) Regulations, January 2021

Table 14: Assumptions and their associated risks

Assumption	*Evidence to support this assumption*	*Risk and mitigations*	*Description of Sensitivity analysis undertaken*
We assume that the draft regulations and the draft code of practice continue to create security benefits throughout the impact assessment period.	The draft regulations are based on a sophisticated threat model which identified the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[108]. The final draft regulations and draft code of practice will have been updated to account for feedback received in a public consultation. Industry feedback will enable effective targeting of the draft regulations and draft code of practice to deliver greatest benefits.	**Medium - Regulations become outdated by technological change.** Technology evolves at pace so new individual security controls would be needed if for example, macro shifts (e.g. mass virtualisation, cloud provision of core) lead to a PECN/S focused framework becoming ineffective. However, future accompanying codes of practice can be updated periodically, subject to consultation. The legislation may also be amended as necessary following parliamentary procedure. Wider DCMS policy planning to address risks of service provision changes and ensure appropriate protections for end-users	The assessment of benefits includes sensitivity analysis to demonstrate the scale of the potential benefits in a low benefit scenario.
We assume that PECN and PECS can pass through security requirements to their suppliers through contractual or other means.	DCMS asked questions on supply chain as part of its survey of PECN and PECS. The majority of respondents thought that some or all of their suppliers would be affected and that the draft regulations would reduce the number of suppliers participating in procurements.	**Low/Medium - PECN and PECS cannot pass on supplier requirements.** We consider that this risk is Low to Medium because those vendors that we have engaged with have indicated that they will comply with	Cost assessment is based on PECN and PECS estimates of direct costs that they will incur for each section of the draft regulations including those on managing the Supply Chain. We estimate an upper and lower bound for all costs impacts We don't estimate wider impacts

[108] https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf

Assumption	*Evidence to support this assumption*	*Risk and mitigations*	*Description of Sensitivity analysis undertaken*
	DCMS also met with a small number of suppliers to discuss the potential cost impact of the draft regulations. This followed a more general round of bilateral engagement with suppliers where DCMS provided a brief history of the rationale behind the security framework and updated on its progress.	the indirect requirements. To mitigate this risk DCMS will maintain review of security improvements to gauge effectiveness of the new framework including as part of the Post Implementation Review. Furthermore, the wider DCMS programme to diversify the supply chain includes de-risking new entrants via a new UK Telecommunications Lab to enable security research and testing.	including the impact of a reduction in the number of suppliers in PECN and PECS procurements. We consider the likelihood of significant market exit to be low given the mitigations set out.
We assume that Ofcom's monitoring regime provides sufficient oversight and that the penalty regime provides sufficient incentive to comply	We asked PECN and PECS questions on how they would comply with the draft regulations in our survey. More than 70% of those that responded said they would comply 'By implementing the requirements set out in the draft code of practice where possible but for some areas we will set out our own approach' The remaining respondents indicated that they would adopt the requirements as set out in the draft code of practice. When asked for the reason for their approach the most popular response was 'to maximise network security'.	**Low - PECN and PECS do not comply with the regulations such that the security outcomes are not achieved.** Ofcom is being provided with significant new oversight powers together with a funding uplift to ensure adequate resources and ability to carry out compliance monitoring. Penalty powers in the Act are among the toughest in comparable frameworks and industry and commentators have noted the 'tough' approach being taken.	We assume 100% compliance in the impact assessment.
We assume that there will be wider benefits than those monetised in this impact assessment.	The benefits monetised in this impact assessment are only those benefits that we have been able to	**Low - no benefits are accrued other than reduced cost to providers of security**	We have not based any analysis on the assumption that more benefits will accrue than those we have

Assumption	*Evidence to support this assumption*	*Risk and mitigations*	*Description of Sensitivity analysis undertaken*
	estimate. The direct benefits monetised are the benefits of reducing the cost of potential security compromises and the indirect benefits monetised are the benefits of unlocking 5G use cases that are reliant on a secure and reliable network. We assume that there will also be wider benefits that have not been estimated. The new security framework is a regulatory intervention that aims to improve security outcomes for the UK's critical national infrastructure. The wider benefits of improved telecoms security include the benefits to consumers of mitigating the likelihood and severity of network outages and data losses, as well as the prevention of threats to telecoms networks that we are not able to predict or anticipate at this stage. For this reason, we assume that the breakeven analysis detailed in section 'Costs and benefits to business calculations' does not fully reflect the proportion of benefits that need to be realised in order to cover costs.	**compromises and the benefit generated by the rollout of specific 5G use cases modelled in the benefits section.** The new security framework is designed to improve security outcomes for the UK's telecoms networks and services, which form part of the country's critical national infrastructure. We consider, therefore, that there are more benefits to society than the savings made by telecoms providers in reduced security compromise costs and the value generated by three 5G use cases of remote medical examination, remote healthcare, monitoring and autonomous cars. Therefore, the risk that there are no additional benefits on top of those monetised is low.	directly estimated. The breakeven analysis detailed in section 'Costs and benefits to business calculations only uses the direct benefits monetised of reduced cost to providers of security compromises. Based on these benefits only, more than 100% of these benefits need to be realised in order to breakeven against the estimated direct costs. If we include the indirect benefits arising from rollout of 5G use cases that are dependent on highly secure and resilient networks, then 44% of total direct and indirect benefits need to be realised to cover the costs (in a low benefit, high cost scenario). Therefore, even if benefits are no higher than those monetised in this impact assessment, total benefits will likely be higher than total costs.

8. Impact on small and micro businesses

Into what sector and/or subsector the affected businesses fall

8.1. In the UK, public communications providers are regulated, primarily, by the Communications Act 2003. Public communications providers include providers of public electronic communications networks (PECN) and providers of public electronic communications networks (PECS).

8.2. Examples of communications providers include[109]:

- Fixed-line owners and providers (such as BT and Virgin Media).
- Mobile network providers (MNOs) (such as Vodafone and O2).
- Companies who use BT's network for their own "indirect access" voice or internet services (using access codes or carrier pre-selection) and wholesale line rental voice and internet services.
- Telecoms resellers providing bespoke services, even though they do not own a network themselves.
- Mobile virtual network providers (such as Virgin Mobile) who do not own their own network but use networks belonging to MNOs to provide services to end customers.
- Internet service providers (ISPs), regardless of the technology they use. They may provide broadband access via: their own fixed-line network (BT); BT's network using ADSL technology (AOL); 3G or 4G mobile; or cable (Virgin Media).
- VoIP (voice over internet protocol) providers (such as Skype).
- Satellite network providers (such as OneWeb).
- Broadcast network providers (such as Arqiva).

Number of businesses in scope of the Regulation

8.3. The requirements set out in the draft regulations will apply to all providers of PECN and PECS, excluding micro businesses irrespective of size, it is vital that the public have confidence and assurance that their communications are secure. Telecommunications services have significant network effects as each additional user increases the connectivity available to all users. This is particularly true of businesses who benefit from increased efficiency and productivity as disparate markets are connected. Therefore, when a security compromise leads to the loss of connectivity for even a small number of consumers, this has wider repercussions for the economy. Further, telecoms networks carry vast amounts of data and so an attack on a small provider can still result in a significant data loss.

8.4. However, the detail of the security expectations should be proportionate, including to the size of the provider, reflecting the different scale of the impact that any security breach or potential loss of services is likely to have. For this reason, the draft regulations include a micro business exemption.

[109] Practical Law; Telecoms Quick Guide, https://uk.practicallaw.thomsonreuters.com/9-503-2464?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

8.5. We do not have a full list of PECN and PECS providers operating in the UK. Our analysis of available information shows that there were approximately 800 providers of PECN and PECS known to Ofcom in 2020.

8.6. We have split these known providers by size according to the number of employees in Table 15, using data on employee numbers from the FAME database, a company information database from Moody's Analytics[110]. Where employee data was not available, we have used total revenue as a proxy measure. This gives an indication of the number of small businesses that are subject to the legislation. However, we note that data on number of employees and revenue is not available for the full dataset. Data is available for 73% of the PECN and PECS providers known to Ofcom; for the remainder we have assumed the same size distribution can be applied. The table shows that there are at least approximately 200 small businesses in our list of PECN and PECS (almost 30%).

Table 15: Estimate of PECN and PECS split by business size

Size	Definition used	Number	% of total number
Large	More than 250 employees (if employee data is unknown, total revenue over £50m)	105	14%
Medium	Between 51 and 250 employees, inclusive (if employee data is unknown, total revenue between £10.2m and £50m)	140	19%
Small	Between 11 and 50 employees, inclusive (if employee data is unknown, total revenue between £362k and £10.2m)	207	28%
Micro	Up to and including 10 employees (if employee data is unknown, total revenue below £362k)	302	40%
Total		752	100%

Note: Business size estimated based on limited data on number of employees and turnover for known PECN/PECS where available.

8.7. In addition to these companies, there may be further PECN/PECS providers who have a relevant turnover of under £5m, do not have Code powers and do not have allocated telephone numbers. These are most likely to be small and micro businesses as they would need to have a relevant turnover of under £5m.

8.8. The draft regulations include a micro business exemption and so micro PECN and PECS providers are not in scope of the draft regulations.

[110] Fame | UK & Ireland Company Data | Bureau van Dijk (bvdinfo.com)

Type of small and micro businesses that will be affected

8.9. As set out in our cost benefit analysis, we consider that type of business is likely to be important in determining the costs of implementing the draft regulations. And that direct costs[111] will be highest for those companies that own and operate their own infrastructure - vertically integrated providers - and the least for resellers who do not own any network infrastructure. Direct costs are more likely to be linked to one off or fixed costs which can have a disproportionate impact on small businesses.

8.10. We do not have a breakdown of PECN and PECS by these categories and we anticipate that many PECN and PECS fall into more than one category. To give an indication of the makeup of small and micro providers we can consider those companies holding Code Powers to provide a proxy for those PECN/PECS that own or operate network infrastructure. This is likely to be an imperfect proxy but we consider it is important for our analysis to distinguish between different types of PECN and PECS.

8.11. We found that a higher proportion of large providers hold Code Powers compared to medium, small and micro providers for whom approximately 20% of PECN/PECS identified hold Code Powers.

Table 13: Breakdown of providers by size and code power status

	With code powers		**Without code powers**	
	Number	**% of size category**	**Number**	**% of size category**
Large	46	44%	59	56%
Medium	29	21%	110	79%
Small	40	19%	167	81%
Micro	60	20%	242	80%
Total	**175**	**23%**	**578**	**77%**

Do the impacts fall disproportionately on small and micro businesses?

8.12. Costs may fall disproportionately on small businesses where the draft regulations create high fixed costs that are incurred regardless of the size of a business. We know that there are both fixed and variable costs required to implement the draft regulations. For example, upgrading of workstations and change management are likely to be variable costs, whereas costs of adjusting contracts with suppliers may be fixed to some degree.

8.13. To understand if this is the case we issued a survey to review the estimated total cost of implementing the draft regulations including seeking data on company size to provide an indication of whether costs are proportionate to company size. Box 4 below provides an overview of our survey.

[111] Indirect costs may be passed through to small and micro businesses but are not included in our cost estimate as set out in section Indirect costs and benefits.

Box 4: Overview of Survey of PECN and PECS

To assess the impacts of the draft regulations we carried out a survey of PECN and PECS the approach to which is set out in section Rationale and evidence to justify the level of analysis. The survey was sent directly to larger providers with whom DCMS is already engaged on the technical detail of the draft regulations. In order to ensure that smaller businesses replied we also distributed a shorter survey aimed at smaller businesses through the Internet Service Providers' Association (ISPA) and the Federation of Communication Services. Before the survey was issued, DCMS 2engaged with multiple trade bodies who were representing a wide range of smaller businesses. This engagement was focussed on the recently published draft SI, seeking views on the technical detail of the draft regulations and identifying where concerns existed.

The survey was completed by 3 small and 3 micro businesses. Given that micro businesses are exempted from the Regulation, we note that this is a small sample of the number of smaller businesses likely to be in the scope of the Regulation.

Further to the survey, we also carried out bilateral clarification interviews with 2 small businesses and 1 micro business. These interviews allowed us to understand the impacts on SMEs at a more granular level.

8.14. Due to the small sample size of the survey, we are not able to split out the data for small and micro businesses. The low number of responses from these businesses may reflect the fact that many of the businesses that accessed the survey do not estimate significant cost impacts from the draft regulations. However, it may also be because a lack of familiarity with the draft regulations made it difficult for these businesses to respond to the survey or that many smaller PECN and PECS were not aware of the survey.

8.15. All providers will have the opportunity to engage with the public consultation. Whilst Tier 3 providers will not be expected to follow all of the measures in the code, it still serves as a best practice guide for them and they will be able to make suggestions on the full range of measures, including implementation timetables. In the period leading up to the public consultation, DCMS continued to engage with smaller businesses through trade bodies and industry-wide events. This engagement process included a roundtable event, jointly run by DCMS and TechUK, focussed on reaching smaller providers who have not previously been engaged with.

8.16. Whilst we are not able to present data on the costs that smaller providers may incur, we note some qualitative findings below.

Box 5: Qualitative findings from Small and Micro businesses

We received three responses to our survey from small businesses and three responses from micro businesses. All of the small businesses that responded are providers who hold code powers, as well as one of the micro businesses. We set out in the section Number and type of businesses that will be affected that we assume these providers will incur higher direct costs than those without code powers on the basis they are more likely to own and operate network infrastructure. This assumption is backed up by the data in the survey responses. The vast

majority of small businesses in scope of the Regulation do not have Code Powers (78%).

Based on the qualitative interviews we found that some key costs for small businesses are:

- Familiarisation costs: Similar to larger businesses, small businesses flagged significant familiarisation costs.
- External costs: A small business is less likely to have internal resources for specialised roles. A number of areas where small businesses would need external resources were highlighted.
- One-off costs: A small business will incur proportionately higher costs for fixed costs. Respondents mentioned some specific areas including testing including external penetration testing and audit costs which may include an element of fixed costs. Other one-off costs noted by small businesses include relocation of services and business process design.
- Ongoing costs: Similar to larger businesses, small businesses expect to incur ongoing costs related to personnel in the security function.

8.17. The survey also helped us to understand the burden of familiarisation costs across all businesses. Given the complexity of the draft regulations and forthcoming draft code of practice, firms indicated that they would incur substantial familiarisation costs.

8.18. For micro and small businesses, which have fewer resources to manage a change, the proportionate burden of familiarisation can be greater. However, based on feedback from the clarification interviews we also found that, due to the complexity of the draft regulations and the size of some affected networks, the costs of dissemination and training were interlinked with familiarisation and were significant for larger businesses. We found that dissemination costs were significant as the draft regulations affect a large number of business units within each organisation such that multiple teams need to understand the draft regulations. We also note that some of the larger businesses were spending significant time engaging on the technical content of the new security framework.

8.19. We also note that in absolute terms the most significant impacts of the draft regulations are likely to fall on larger businesses. This is in part due to the difference in size of the smallest and largest providers. It is useful to note that the seven largest providers hold 88% of the total fixed telecoms market in the UK. In the mobile network, this is even more pronounced, with just four network providers making up circa. 85% of the mobile network. The market share of each of these providers are shown in tables 16 and 17.

Table 16: Mobile network market shares by subscribers at 31 December 2017

Provider	**Market share**
BT / EE	28%
O2	26%
Vodafone	21%
Three	12%
Tesco Mobile	6%

Provider	Market share
Virgin Mobile	4%
TalkTalk	1%
iD Mobile	1%
Sky	1%
Others	<1%

Source: Statista[112]

Table 17: Fixed network market shares by broadband subscribers at 2018

Provider	Market share
BT	35%
Sky	23%
Virgin Media	20%
TalkTalk	11%
Others	12%

Source: Statista[113]

8.20. The vast majority of UK telecoms networks are owned and managed by the nine providers above, all with a turnover above £5m. Therefore the large providers will be the ones who have to bear the majority of the costs involved in making the necessary changes to comply with the legislation.

8.21. In summary, our survey did not reach a representative sample of SMEs and we are therefore unable to conclude on the impact of size of business on cost of implementing the draft regulations.

8.22. Whilst we do not have data on the expected cost impact by firm size, we have considered the make up of small businesses that we have identified in the scope of the legislation. We found that these providers were less likely to hold Code Powers than large and medium providers and this may reflect the type of business with smaller numbers of SMEs operating network infrastructure. However, there are likely to be a number of SMEs who do incur significant costs, including indirect costs, as a result of the draft regulations and we consider both exemption and mitigation below.

Could SMBs be exempted while achieving the policy objectives?

8.23. In the 'Better Regulation Framework' government has committed to considering whether the impacts of regulatory changes will fall disproportionately on small and micro businesses and whether such businesses could be exempted from the draft regulations, or the impacts mitigated in some way without compromising the policy objectives. The guidance sets out that the default option is to exempt small and micro-businesses from the requirements of new regulatory measures. Where exemption is not possible consideration should be given to whether burdens could be mitigated or minimised.

112 UK: Mobile network market share 2018

113 UK telecoms providers: broadband subscribers share 2018

8.24. For small businesses, we do not consider an exemption to be appropriate. Customers of telecoms providers deserve appropriate levels of security to apply to their communications services irrespective of the size of the company providing the communications network and/or services.

8.25. For micro businesses we consider that an exemption is appropriate. This is because there exists the possibility of a disproportionate financial impact on micro businesses for applying the requirements, whilst their networks present minimal risk to national security. While the survey responses from micro businesses were limited in number, the received responses suggest a higher cost incurred as a percentage of turnover for micro businesses compared to small businesses. The disproportionate financial impact on micro businesses primarily comes from higher relative fixed costs, limited in-house technical expertise and higher relative familiarisation costs. Therefore, the Statutory Instrument will include an exemption for micro businesses.

Could the impact on SMBs be mitigated while achieving the policy objectives?

8.26. There are many different sized telecoms companies providing telecoms networks and services, and while their security and resilience is critical, it is important their differences are recognised.

8.27. To ensure measures are applied proportionately, the government intends to define three tiers of telecoms provider in the initial draft draft code of practice, which will be finalised via public consultation. The consultation will set out the details of the approach to tiering; at this stage we expect that small businesses will fall into Tier 3.

8.28. A summary of the obligations of each tier and the level of oversight applied is below:

- The draft code of practice will apply to the largest national-scale ('Tier 1') telecoms providers, whose availability and security is critical to people and businesses across the UK. These providers will also be subject to intensive Ofcom monitoring and oversight.
- The draft code of practice will also apply to medium-sized ('Tier 2') telecoms providers, who will be subject to some Ofcom oversight and monitoring. These providers are expected to have more time to implement the security measures set out in the draft code of practice.
- The smallest ('Tier 3') telecoms providers, including small businesses, will need to comply with the law. It is not anticipated that the draft code of practice will be applied to Tier 3 providers, but these providers may be subject to some limited Ofcom oversight.

8.29. A disproportionate impact on Tier 3 providers, and thus on small businesses, is expected to be mitigated by no expectation to follow the detailed requirements set out in the code and a proportionality requirement which is built into the Act and limited oversight from Ofcom. In addition to this, under Option 4 Tier 2 providers would have a longer implementation timetable and this could have an impact on both when these providers begin to incur costs and the level of costs they will incur. Tier 3 providers may choose to adopt the measures in the draft code of practice where these are relevant to their networks and services. We welcome feedback from providers who may be considered Tier 3 on whether further specific guidance is needed to assist compliance with legal obligations.. We will seek to understand the degree to which this implementation delay impacts costs in the survey issued alongside this consultation.

8.30. We do not anticipate that Ofcom will require Tier 3 providers to undertake any periodic reporting under this legislation. While Tier 1 and Tier 2 providers will likely be expected to produce annual reports of their compliance against the legislation and any deviation from the draft code of practice, this will not be expected of Tier 3 providers. According to the Deloitte report of the impact of FCA regulations on financial services firms, activities where small firms would save more cost than medium/large firms if rules were removed includes periodic reporting[114].

8.31. Given the reduced level of obligation and oversight placed on Tier 3 providers, we anticipate that the disproportionate impact of the new framework on small businesses will be mitigated. As noted, the impact on micro businesses will be mitigated by the inclusion of a micro business exemption in the legislation.

[114] The cost of regulation study, Deloitte, June 2006

9. Wider impacts

9.1. In this section we consider the wider impacts of the Act and the draft regulations. We focus on the wider impacts on telecommunications providers through impacts on competition (which we assess through the competition assessment checklist) and wider incentives and behaviours - in particular enabling or restricting innovation - as part of our competition assessment.

Competition assessment

9.2. In line with the competition impact assessment guidelines we have considered whether the new security framework is likely to have an impact on competition by considering whether the legislation will:

- Directly or indirectly limit the number or range of suppliers
- Limit the ability of suppliers to compete
- Limit suppliers' incentives to compete vigorously
- Limit the choices and information available to consumers

9.3. We consider these questions in turn, first noting the market structure of the downstream UK telecommunications markets. We find that the draft regulations will not limit the number or range of suppliers, or their ability to compete for the choices and information available to consumers.

9.4. The scope of our competition assessment is the downstream telecommunications market because this is the market to which the draft regulations apply. We expect that the upstream telecommunications market will be indirectly affected where downstream providers pass on requirements to their suppliers through contractual or other means. These impacts are set out in the section on Indirect costs and benefits.

Downstream UK telecommunications market

9.5. In the UK mobile sector there are four mobile network providers ("MNOs"), Vodafone, EE, O2 and Three, as well as numerous MVNOs (mobile virtual network providers). MVNOs do not own the networks they use and instead purchase wholesale services from MNOs, as a result they are less impacted by the legislation where this would apply to their wholesale provider's network.

9.6. The UK fixed telecoms sector is composed of network providers operating at national and regional-only levels. BT Group has historically been the largest fixed network provider in the UK, given its ownership of a comprehensive network (in geographical terms) within the UK. BT's 'final-mile' fixed access network, Openreach, is legally separated from BT Group, and provides wholesale access services to other fixed telecoms service providers.

9.7. In addition to BT, Virgin Media operates a cable network that currently covers approximately 50% of the UK. In addition to BT and Virgin Media, there are many fixed telecoms retail service providers in the UK, including Sky and TalkTalk, along with various alternative infrastructure providers, including Hyperoptic, Gigaclear, KCOM and CityFibre who provide retail and/or wholesale services in discrete geographical areas.

Will the legislation limit the number or range of suppliers?

9.8. The draft regulations do not directly limit the number or range of suppliers in the downstream telecommunications market. However, the Competition Assessment guidelines note that "a competition assessment should assess whether the proposals may indirectly limit the number or range of suppliers in a market. A proposal could have this effect if it:

- significantly raises the costs of incumbent firms, causing them to exit the market;
- significantly raises the costs of new suppliers (including small businesses) relative to existing suppliers; and
- significantly raises the costs of some existing suppliers relative to other existing suppliers."[115]

9.9. We therefore consider each of these questions.

Will the legislation raise the costs of incumbent firms?

9.10. The draft regulations will raise the height of the security bar and require telecoms providers, overseen by Ofcom and government, to design and manage their networks to meet the new duties. The draft code of practice will provide clarity to industry on what is expected in terms of network security.

9.11. We have found that the draft regulations will create significant costs for some providers and these include one off costs in adjusting business processes and, for example, altering contracts as well as ongoing costs.

9.12. Large and medium sized providers that responded to our survey estimated potential one off costs of 8.4% of turnover and annual ongoing costs of 2.5% of complying with the draft regulations on average. Although we expect that this will vary by type of provider. However, we also expect that implementing the draft regulations will deliver direct benefits to providers reducing the net cost.

9.13. It is not expected that this legislation would affect the number of these incumbent networks because - despite the costs identified - the providers required to implement the full draft code of practice are large organisations who already have significant security and resilience functions and have the capacity to implement the requirements. Additionally, the NCSC has consulted with these providers on their guidance - on which the code will be based - in draft version to ensure that they can be implemented by providers.

9.14. The impact on small and micro businesses will be mitigated as set out in Impact on small and micro businesses. Given these mitigation measures, the impact on small and micro businesses is expected to be lower than on large and medium sized providers.

Will the legislation raise the costs of new suppliers

9.15. We have also considered whether new suppliers might be affected more - relative to incumbent suppliers.

9.16. We note that the costs of implementing the draft regulations appear to be skewed towards one off costs. This could be indicative of significant change management processes and costs associated with changes to existing business processes and

[115] Competition impact assessment Guidelines, Section 3.24.

systems. These types of costs might affect new suppliers less as the draft regulations can be built into business process and system design from the outset.

9.17. This is borne out through qualitative feedback which indicated that some key drivers of the costs of implementing the draft regulations involve changes to existing processes or systems. For example:

- the impact of implementing changes in legacy equipment
- the impact of implementing changes outside of the normal replacement cycle for equipment
- making changes to contracts with third party suppliers
- change to business processes

9.18. We consider that whilst the costs of implementing the draft regulations will apply equally to existing providers and potential entrants, they could be higher for existing providers who have legacy systems as well as equipment that is not considered legacy but will require an update outside of normal replacement cycles.

9.19. We therefore consider the impact on new suppliers is unlikely to be higher than existing suppliers - in relative terms.

Relative impacts on existing suppliers

9.20. We have considered whether the draft regulations will significantly raise the costs of some existing suppliers relative to other existing suppliers. First we note that the draft regulations affect a wide range of different providers ranging from vertically integrated suppliers to resellers who may not own any network infrastructure. We expect the costs of implementing the draft regulations to vary according to these provider types and that - in general - providers who own more network infrastructure will incur higher costs. However, those providers who incur lower direct costs are likely to incur indirect costs as their suppliers - infrastructure owners - pass through the costs of compliance with the draft regulations.

9.21. Another area where relative impacts may differ is in terms of scale of provider. We are aware that smaller networks may be disproportionately affected due to the element of fixed costs in implementing the draft regulations. Examples of costs that include an element of fixed costs are the costs of familiarisation and renegotiating contracts with suppliers. These impacts are discussed in the Impact on small and micro businesses section of this Impact Assessment.

9.22. In particular, option 4 mitigates the costs in implementing the draft regulations for smaller providers by delaying their implementation date by two years. This delay means that smaller telecommunications providers would be able to either delay implementation by two years or implement over a longer period. We will explore further how the delay to the implementation period would affect smaller providers through the survey issued alongside this consultation including whether it reduces their costs of implementation and how this affects their average costs relative to other providers.

9.23. We have also considered the relative impact on suppliers who are global providers. These suppliers may find it more difficult to implement UK-specific draft regulations where they differ from standards in other countries.

9.24. However, we note that a large number of suppliers operate globally yet still meet the needs of specific markets and serve a vast array of providers, many of whom have different needs. Global suppliers are likely to assist providers to meet legal requirements

as far as possible. In the global context, we note that the draft regulations are innovative in setting out security requirements for telecommunications providers in detail. However, other countries are planning similar measures, as noted in section 5, which will impact on the market globally, reducing any barrier to entry into the UK market that the new security framework may create.

Will the new security framework limit the ability of suppliers to compete or compete vigorously?

9.25. The draft regulations and draft code of practice will provide a 'floor' not a 'ceiling'; providers will be encouraged to exceed them and constantly innovate to enhance security.

9.26. The legislation will, however, standardise the basic level of security provided by network and service providers. If security is a feature of competition between providers this could decrease the degree to which providers compete or lead them to compete in other ways.

9.27. The Review found that there are a lack of commercial drivers for providers to put in place good cyber security because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality. This indicates that providers are not currently competing on security features of their networks; and that the standardisation of security is unlikely to affect levels of competition.

Impact on innovation

9.28. It is important to consider the impact of policy on innovation. In particular:

- consider the impact of their policy on innovation throughout the regulatory cycle;
- consider the impact of innovation on their policy throughout the regulatory cycle;
- design and deliver more flexible and agile policies (where appropriate); and explain how they have used evidence in doing this.

9.29. In addition to this the security framework has been designed to balance the need for a level of prescription in setting out the security requirements with a mechanism for providers to follow their own approach to implementing the draft regulations.[116] This approach recognises the need to balance the potential benefits of providers being able to innovate and react to change against the need to meet a level of security requirements.

9.30. In our survey of PECN and PECS we asked providers how they plan to comply with the draft regulations. Only 14% expected to comply by implementing the code in all areas; the vast majority indicating that they would depart from the code in some way.

9.31. A follow up question asked those respondents who had indicated that they would set out their own approach in some areas why that was the case. The responses are set out in full below:

[116] Note on the role and status of the draft code of practice: If a provider decides to depart from the Code where it applies to them, this would not necessarily put them in breach of their duties (as per the new section 105H of the 2003 Act which would be introduced by the Telecommunications (Security) Bill). However, under new section 105I of the 2003 Act, where Ofcom has reasonable grounds for believing that a provider is failing, or has failed, to act in accordance with this guidance where it applies to them, Ofcom may direct them to explain the reasons for the failure.

Table 18: Q2.3b - If you plan to implement the requirements set out in the draft code of practice where possible but plan to set out your own approach for some areas, please select the reason(s) for this approach.

Answer	%
Difficult to implement requirements set out in the draft code of practice due to legacy systems	20%
To be more cost-effective	23%
To maximise network security	20%
To align with our company's global approach	14%
We prefer another approach, please explain	23%

9.32. These responses indicate that providers will utilise the flexibility afforded by the draft code of practice for a variety of reasons including preference for another approach. Where providers have indicated that they would follow the code in order to comply with the draft regulations the most common reasons were to maximise network security or the chances of full compliance.

9.33. In summary we consider that the draft regulations and the supporting code will not limit the ability of suppliers to compete because the code provides an inherent level of flexibility. We also note that security does not appear to be a key driver of competition.

Will the new security framework limit the choices and information available to consumers?

9.34. We do not expect this legislation to have any impact on the number of suppliers and so impact consumer choice.

9.35. We expect that the new security framework could increase the level of information available to consumers rather than limit it. This is because it is possible that standardising security levels could create a standard that is more visible to consumers. The draft regulations will mean that consumers can expect a standardised minimum level of security from the telecommunications networks and services that they use. Providers could use the draft code of practice to communicate with their customers that they comply with a security standard.

Equalities Impact Assessment

9.36. We do not consider there to be any disproportionate impacts to groups with protected characteristics. The costs of this legislation fall on businesses only so do not have an impact on any protected groups. The benefits to society arise from the reduction in the impact of security compromises for telecoms providers. This is likely to benefit any consumer in the UK with access to a mobile or broadband service. This does not preclude any protected groups since every home and business in the UK has the legal right to request a decent, affordable broadband connection under the Broadband Universal Service Obligation (USO)[117]. The benefits accruing from the deployment of 5G use cases that require a reliable and secure 5G network is expected to accrue mostly to businesses. While a small proportion of consumers have access to 5G already[118], it is widely considered that the majority of 5G benefits will accrue to businesses. While consumers will benefit from faster speeds, more availability and consumer-focused use cases such as smart home IoT devices, the real gains come from the benefits of increased efficiency and productivity in almost every sector. As such, we do not consider protected groups to be either positively or negatively impacted by this legislation compared to the UK population as a whole.

9.37. It is worth noting that a small proportion of the UK are digitally-excluded. According to Ofcom's latest 'Adult's Media Use and Attitudes' report, 6% of households did not have access to the internet at home as of March 2021 and a further 1% of adults aged 18+ had access to the internet at home but did not use it. In particular, the groups more likely not to have internet access at home – and therefore, to be more at risk of digital exclusion – were those aged 65+ (18%), those in DE households (11%) and those who were most financially vulnerable (10%)[119]. However, we do not consider that this legislation is increasing the disadvantage of those who are digitally excluded. The outcome of the policy is ensuring the security and resilience of the existing and future telecoms networks in the UK. While we expect the legislation to enable the growth of a number of 5G use cases, the benefits of these fall on businesses rather than consumers for the most part and so would not further disadvantage those who are digitally excluded.

[117] In March 2018, the UK government introduced legislation for a Broadband Universal Service Obligation (USO), which will give eligible homes and businesses the right to request a broadband connection that delivers a decent broadband service of at least 10 Mbit/s download speed and 1 Mbit/s upload speed. This came into force in March 2020. The Universal Service Obligation (USO) for Broadband - House of Commons Library (parliament.uk)

[118] 5G services available at around 3,000 sites. EE, O2, Three and Vodafone first started rolling out 5G in the UK in 2019 and have continued to extend their networks across the UK. Many 5G sites are in busy areas and are providing enhanced capacity to existing mobile data services. Of all 5G sites that have been deployed, 87% are in England, 7% in Scotland and 3% in both Wales and Northern Ireland. This split broadly reflects the national distribution of all mobile traffic across the UK. Connected Nations report 2020, Ofcom

[119] Adult's Media Use and Attitudes report 2020/21 (ofcom.org.uk)

10. A summary of the potential trade implications of measure

Impact on trade: network and service providers

10.1. The draft regulations currently include requirements intended to mitigate the risk to the availability of telecoms networks in the event of disruption to international connectivity or offshore technical and operational support.

10.2. They also seek to address specific security risks arising from certain security functions (including people, equipment and stored data) being offshored. These are not yet finalised but were included in the early draft regulations to seek providers' views and ensure that any final requirements are appropriate and proportionate to the scale of risk against impacts.

10.3. The intent of the draft regulations is to ensure that there is always the ability to operate and control UK networks within the UK, and that decision making relating to UK networks involves UK oversight. The draft regulations aim to ensure UK networks remain available, particularly in the event of any impact to international connectivity, as well as limiting the ability for malicious insiders, based outside the UK, to damage UK networks.[120]

10.4. The following duties on providers are included in the early draft regulations published in January 2020:

- 'to ensure that the network provider is able to assess risks to, and where necessary maintain the operation of, a public electronic communications network located in the United Kingdom, without reliance on persons, equipment or stored data located outside the United Kingdom.[121]
- to ensure that tools enabling monitoring or audit cannot be accessed from outside the United Kingdom if they enable monitoring or audit (i) in real time, or (ii) of the content of signals.[122]
- to avoid dependence on persons, equipment or stored data located outside the United Kingdom to monitor and audit the use of networks located in the United Kingdom.[123]
- to acquire, and retain within the United Kingdom, offline and online copies of information necessary to operate security critical functions, and, so far as is proportionate, a copy of information necessary to operate parts of the networks other than security critical functions'.[124]

10.5. There are a number of sections in the draft code of practice that will set out more detailed guidelines relating to the above.

10.6. Amendments to the requirement for UK-based monitoring and auditing capabilities in draft regulations 4 and 5 of the January 2021 draft regulations could reduce costs for providers who currently offshore these functions.These amendments, if taken forward,

---

[120] Summary of the NCSC's security analysis for the UK telecoms sector, 2020, Paragraph 7.6.

[121] Draft Electronic Communications (Security Measures) Regulations - GOV.UK (www.gov.uk), section 3, point 3(f).

[122] ibid, section 4, point 3(f)

[123] ibid, section 5, point 3(h)

[124] ibid, section 8, point 2(a)

would only prevent monitoring and auditing functions from being accessed and located from a narrow set of countries.

10.7. In weighing the final approach, the government is aware of the potential for any draft regulations to impose additional obligations on foreign businesses where security functions are not currently in the UK, or those global providers headquartered in the UK who nevertheless may have some security functions or critical support based overseas. Any impacts may be more limited for network providers only serving the UK market although outsourced functions may also create impacts for these providers. The final regulations will take these impacts into account.

10.8. The final stage impact assessment that will be published alongside the final Regulations will take account of any responses that raise international investment implications arising from the measures. This will be considered in the context of the dependency of 5G and full fibre network rollout on such inward investment

Impact on trade: third party suppliers

10.9. Providers who are subject to the new security framework will be required to use network equipment suppliers and third party suppliers who can meet specific security requirements. This relates both to goods and services provided by these suppliers. There is no estimate for the proportion of vendors serving the UK telecoms market that would currently meet these requirements. However, we do not expect the legislation to have a significant impact on trade as the legislation gives no advantage for domestic vendors over foreign vendors.

11. Justice impact test

11.1. Ofcom will be given an expanded security duty to regulate the security framework, taking regard of the draft code of practice in their regulatory work.

11.2. Providers will be required to provide regular reporting to Ofcom on the steps taken to comply with their statutory obligations. Ofcom would also have the ability to conduct inspections and validation testing to confirm the information provided by providers is accurate.

11.3. Ofcom will have a range of penalties to ensure compliance with this system, these will include financial penalties and a direction power. This will mirror Ofcom's current penalties as set out in Communications Act 2003. However, some penalties will be increased and this has been set out in a Justice Impact Assessment which was approved by the Ministry of Justice in February 2021. The current appeals system will be utilised.

11.4. As set out in the existing legislation, Ofcom must apply these penalties proportionately and appropriately, and allow representations from providers.

12. Monitoring and evaluation

12.1. A methodological approach for the post-implementation review, including counterfactual, key metrics, evaluation criteria and timelines is being finalised by DCMS. An agreed evaluation will likely utilise evidence from multiple industry surveys, in addition to policy implementation data from Ofcom highlighting compliance metrics. DCMS will consider top down evaluation metrics, such as the number of incidents reported and the number of 5G and full fibre network rollouts. It should be noted however, that such top down data may lead to misleading conclusions of the true effect of the draft regulations. This is due to the difficulty in correctly identifying the impact of the draft regulations on trends such as the increasing number of cyber security incidents as well as 5G and full fibre rollout. The final impact assessment will expand on the evaluation strategy to assess whether the policy has met its objective and seek to provide additional information on how the draft code of practice and draft regulations will continue to be deemed fit-for-purpose. The review of estimated impacts and key assumptions will be measured against the objectives of the Telecommunications (Security) Act as well as the DCMS outcomes plan.

How is the current system monitored

12.2. Ofcom has the following powers with respect to monitoring public communications providers under legislation currently in force:

- Ofcom may require providers of PECN and PECS to submit to, and pay for, an audit of the measures they are taking to comply with the obligations; and
- Ofcom can use the information gathering and enforcement provisions in the Communications Act to investigate, rectify, and penalise any infringement of these obligations.

12.3. In addition, providers of PECN and PECS have a statutory obligation to report to Ofcom breaches of security which have a significant impact on the operation of the network or service. Providers of PECN also have an obligation to report reductions in the availability of a network which have a significant impact on the network to Ofcom.

12.4. The guidance that is currently published by Ofcom to guide communications providers on their security and resilience obligations has been updated once since its publication in May 2011.[125]

12.5. With reference to the updated guidance, Ofcom notes that 'Because of the dynamic nature of the telecoms market, and the changing threats to security and resilience it faces, we will continue to review this document regularly, and if required, update it again.'[126]

[125] Ofcom's current guidance security requirements in sections 105A to D of the Communications Act 2003 was published in 2017. This guidance replaced previous guidance which was published in May 2011.
[126] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance

What external factors will impact on the success of the new telecommunications security framework

12.6. The new telecoms security framework is being put in place against a backdrop of our increasing reliance on telecoms networks for our daily lives. New technologies are expected to transform how we work, live and travel providing opportunities for new and wide-ranging applications, business models, and increased productivity. Increased reliance on these new networks will increase the potential impact of any disruption and means there is a need to reassess the security framework.

12.7. As set out in the section 5G and full fibre networks must be secure and resilient, the move to 5G brings a new dimension to the security risks, given the greater dependence that wider UK critical national infrastructure (CNI) is likely to have on UK telecoms than is the case with 3G/4G.

12.8. In the Review the NCSC concluded that 'if new 5G use-cases emerge at scale, a successful cyber attack could be highly disruptive across UK CNI and the wider economy.'[127] Such changes in technology or the adoption of technology can rapidly change the security landscape of the telecommunications sector.

12.9. The Act provides the Secretary of State with powers to issue new and revised codes of practice and withdraw codes of practice. These powers can act as a tool to amend the duties on providers if technological changes result in changes in the security landscape. Before issuing new draft code of practice or amending existing codes of practice, the Secretary of State must publish a draft of the new or revised code and consult with Ofcom and PECN/S providers to whom the new code would apply.

12.10. The final Regulations will be reviewed at least once every five years as outlined in section 14 of the Act. The final Regulations may be updated on a more regular basis than this to reflect changes in policy in response to the emergence of specific new threats or to address security vulnerabilities identified through compliance reporting. The government will discuss any such changes to legal obligations with the industry before they are implemented.

How will the new security framework be monitored

12.11. The new security framework will include a set of security duties in the Communications Act 2003, a set of regulations and a code of practice.

12.12. The contents of the code of practice will be reviewed on a regular basis to ensure it keeps pace with the latest threats and evolving technology.

12.13. The NCSC will inform the government of where new threats and vulnerabilities lie based on its analysis and classified intelligence.

12.14. Alongside this, Ofcom must publish a security report after the end of each reporting period containing information and advice that Ofcom considers will assist the government with forming policy. This will include information about whether providers have complied with their duties under the Act and acted in accordance with the code. Access to this information will allow the government to understand how well the new framework is working and where changes to the code need to be made.

12.15. Box 6 below sets out an extract from the Telecommunications (Security) Act which amends the Communications Act 2003 to add section 105Z 'OFCOM reports on security'.

[127] The Review, page 24.

This section sets out the contents of the security report that Ofcom must prepare and send to the Secretary of State.

Box 6 - Extract from the Telecommunications (Security) Act: Section 11 (2)

105Z OFCOM reports on security

(1) As soon as practicable after the end of each reporting period OFCOM must prepare and send to the Secretary of State a report for the period (a "security report").

(2) A security report must contain such information and advice as OFCOM considers may best serve the purpose mentioned in subsection (3).

(3) The purpose is to assist the Secretary of State in the formulation of policy in relation to the security of public electronic communications networks and public electronic communications services.

(4) A security report must in particular include—

(a) information about the extent to which providers of public electronic communications networks and public electronic communications services have complied during the reporting period with the duties imposed on them by or under sections 105A to 105D, 105I to 105K, 105N(2)(a) and 105O;
(b) information about the extent to which providers of public electronic communications networks and public electronic communications services have acted during the reporting period in accordance with codes of practice issued under section 105E;
(c) information about the security compromises that OFCOM have been informed of during the reporting period under section 105K;
(d) information about the action taken by OFCOM during the reporting period in response to security compromises they have been informed of under section 105K;
(e) information about the extent to which and manner in which OFCOM have exercised the functions conferred on them by sections 105I and 105L to 105V during the reporting period;
(f) information about any particular risks to the security of public electronic communications networks and public electronic communications services of which OFCOM have become aware during the reporting period;
(g) any other information of a kind specified in a direction given by the Secretary of State.

12.16. This report will include a range of information including compliance with the new security framework but also information on the number of security compromises that Ofcom have been informed of during the reporting period.

12.17. Where changes are proposed to codes of practice, the government will consult on the draft updated codes before they are introduced. Where targeted and specific threats emerge the NCSC may issue guidance to relevant providers, to prevent significant damage to UK networks and services.

12.18. Finally, the legislation places a new duty on telecoms providers to undertake a review at least once a year of the risks of security compromises to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises occurring. This will provide a useful view on the effectiveness of the legislation in improving security outcomes.

12.19. A Post Implementation Review of the Telecommunications (Security) Act will take place by October 2027; the review will assess whether the new security framework:

- has achieved its original objectives;
- has objectives that remain appropriate;
- is still required and remains the best option for achieving those objectives; and
- could be achieved in another way which involves less onerous regulatory provision to reduce the burden on business and/or increase overall societal welfare.

12.20. The Review will be informed by all of the data sources set out above. This will include data collected by Ofcom on compliance with the code of practice which will provide DCMS with information on how Tier 1 and 2 providers are implementing the code and data on security compromises reported. DCMS is also commissioning a piece of market research to understand the characteristics of telecommunications providers in the UK including their size, structure and activities. This research will help us to understand more about tier 3 providers, which is the group with the lowest response. Where required DCMS will seek additional data.

13. Glossary and Abbreviations

3PA - Third Party Administrator: MSPs, operator group functions, or external support for vendor

5G - Fifth generation technology standard for mobile networks and is the planned successor to 4G and previously 3G networks

AR - Augmented reality

ADSL technology - Asymmetric digital subscriber line technology

CA - Communications Act 2003

CNI - Critical National Infrastructure

DCMS - Department for Digital, Culture, Media & Sport

FTTP - Fibre to the premises

GVA - Gross value added

HRV - High risk vendor

IoT - Internet of things

ISPA - Internet Service Providers' Association

MANO - Management and Organisation

MNO - Mobile Network providers

MSP - Managed Service Provider: A third-party that helps to run or administrate your network. equipment (e.g. third-line support function).

MVNO - Mobile Virtual Network providers

NCSC - National Cyber Security Centre

NFV - Network Function Virtualisation

NFVi - Network Function Virtualisation Infrastructure

NSA - Non-standalone

Ofcom - Office of Communications

PAW - Privileged Access Workstation; Workstations through which Privileged Access is possible.

PECN - Public Electronic Communications Network

PECS - Public Electronic Communications Service

SA - Standalone

VoIP - Voice over IP

Annex 1 - Methodology behind benefits analysis of 5G use cases

Remote medical examination (Economic Benefit: £8.5bn)

1.1. The Ericsson report states the key dimensions of 5G in enabling remote medical examination and monitoring:
- 'Enabling high definition video streaming over mobile networks
- Offering high enough availability and reliability to constantly monitor critical patient health parameters
- Being secure enough to adhere to sensitive patient data regulations'[128]

1.2. A 2019 report from Cambridge Wireless states that '5G technology brings the opportunity for paramedics to transmit images, data and detailed information from ambulances *en route* to the hospital to prepare doctors for treatment. Equally, high-quality video links may allow paramedics to conduct emergency treatment or assess and diagnose patients at the scene with the assistance of an on-line specialist.'[129]

1.3. O2 published a report on the value of 5G in May 2018 ('the O2 report'), which estimates that high quality and secure tele-health video conferencing will allow people to conduct GP consultations from their smartphone or other smart devices. This will save individuals an estimated 3.3 hours per year, saving £1.3bn in lost productivity through workplace absence[130]. The NHS Long Term Plan, published in January 2019, states that 'over the next five years, every patient will have the right to online 'digital' GP consultations, and redesigned hospital support will be able to avoid up to a third of outpatient appointments - saving patients 30 million trips to hospital, and saving the NHS over £1 billion a year in new expenditure averted.'[131]

1.4. The development of remote healthcare is of even higher importance due to the Covid-19 pandemic. This has led to a faster uptake of remote medical examination than anticipated. Recent data collected by the Royal College of GPs showed that at the peak of the pandemic, up to 70% of consultations were carried out by phone or video call[132]. Reliable, 5G mobile networks are the catalyst for this remote approach to continue and evolve. For example, 5G-aided remote CT scans were used to diagnose COVID-19 patients in China[133].

1.5. Analysts at Global Market Insights predict the use of telehealth will triple by 2025, fuelled largely by 5G[134]. The same report states that the 'Teleconsultation service market is expected to grow at 18.9% CAGR across the forecast timeframe.'[135]. This does not account for the acceleration enabled by Covid-19. We have based

[128] Ericsson's 5G Business Potential report
[129] How 5G Could Transform the Delivery of Healthcare
[130] The value of 5G for cities and communities
[131] NHS Long Term Plan v1.2 August 2019
[132] Around 7 in 10 patients now receive GP care remotely in bid to keep patients safe during pandemic, says RCGP, 30 April 2020
[133] 5G-aided remote CT scans used to diagnose COVID-19 patients, 28 February 2020
[134] Global Telemedicine Market size to exceed $130.5 Bn by 2025
[135] Telemedicine Market By Service Type, Component and Deployment | Forecast 2023

our analysis on pre-Covid figures as the growth rates due to Covid are not fully established.

1.6. Our model of the economic benefits of remote medical examination starts with the £1.3bn benefit expected in 2026. This is based on the assumption that 5G penetration will be close to 100% in UK cities by 2025 from the O2 report. We have then applied the one year delay to rollout assumed for Covid to model the optimistic scenario. Since many of the draft regulations will have mostly been implemented by Tier 1 providers by 2024, we have assumed that the benefits will begin to accrue in 2024, increasing linearly from £0 in 2023 to £1.3bn in 2026. Beyond 2026, we have assumed the 18.9% CAGR growth rate reported above. The central and worst case scenarios delay these benefits across the impact assessment period by a further 2 and 4 years respectively.

Remote health monitoring (Economic Benefit: £8.9bn)

1.7. In the context of the Covid-19 pandemic, much attention has focused on 5G's potential to support telehealth services. 5G offers the potential of moving these interactions a big step forward by, for example, adding sensors and virtual reality to teleconferencing, enabling healthcare workers to remotely monitor vital signs during calls. 5G can transmit sizeable data packages, testing patients with conditions for changes in their heartbeat, blood sugar and blood pressure multiple times a day using cloud-linked scanners[136].

1.8. The O2 2018 report estimates that health monitoring devices will reduce hospital readmissions by 30% by 2025 and save £463m in NHS costs as a result (through a combination of decreasing bed occupancy and giving hours back to hospital staff). Remote health monitoring will also save local councils £890m through reduced social care budgets[137]. Taken together, this produces a potential annual benefit of £1,353 million by 2025[138]. This is a lower estimate than the one produced in the 2017 study by the Iqvia Institute for Human Data Science, which states that the use of Digital Health apps could achieve annual cost savings of £2 billion[139].

1.9. A Deloitte report in 2018 estimated that the Internet of Medical Things market - defined as medical devices that can generate, collect, analyse, transmit and store large amounts of health data - is expected to grow at a compound annual growth rate (CAGR) of 30.8% from 2017 to 2022[140].

1.10. Our analysis of the economic benefits of remote medical monitoring starts with the £1.3bn benefit expected in 2026, based on the O2 report with a one-year delay for Covid impacts. Again, this forms the basis of the optimistic scenario. We have made assumptions on benefit growth consistent with the remote medical examination use case above (a more conservative growth rate than the Deloitte CAGR estimate).

---

[136] 5G in healthcare, PwC, 2020

[137] The value of 5G for cities and communities

[138] The value of 5G for cities and communities

[139] The Growing Value of Digital Health in the United Kingdom

[140] Medtech and the Internet of Medical Things How connected medical devices are transforming health care

Autonomous cars (Economic Benefit: £3.8bn):

1.11. TechRadar stated in June 2019 that '5G could be the key to making self-driving cars commonplace. For them to work most effectively they need to be able to rapidly send and receive data to and from other cars, smart roads and more, which requires a speedy network, low latency, lots of bandwidth and high reliability. 5G promises all of that.'[141]

1.12. A 2017 publication from the Centre for Connected and Autonomous Vehicles) published in July 2017 estimates that the GVA created in the UK by the autonomous car industry will be £3.4bn in 2025, growing to £5.6bn in 2030. The internationally recognised standard for automated driving defines six levels of driving automation, from "no automation" (Level 0) to "full automation" (Level 5). The key distinguishing factor for levels 3 and above is that when the system is engaged, the full dynamic driving task can be undertaken by the vehicle. We consider 5G to be a requirement for this level of automation. Only autonomy levels 3-5 are considered in this study for the purposes of economic analysis.

1.13. Based on our assumption in the optimistic scenario that 5G will be fully deployed by 2026, we have modelled a £3.4bn annual benefit in 2026, growing at a linear rate to £5.6bn in 2031. In the central scenario, we have assumed these benefits have been delayed by a further 2 years. In the worst case scenario, we have modelled no benefits occurring from autonomous cars as they would not be deployed within the impact assessment period. No benefits are assumed to be accrued before 5G is fully rolled out in any scenario.

[141] 10 things 5G can do that 4G can't