Title: The Telecommunications Security Bill 2020: The Telecoms Security legislation **IA No:** **RPC Reference No:** **Lead department or agency:** Department for Digital, Culture, Media and Sport **Other departments or agencies:**	**Impact Assessment (IA)** **Date: 09 June 2020** **Stage: Final** **Source of intervention: UK Government** **Type of measure: Primary legislation** **Contact for enquiries:** Essie Barnett essie.barnett@culture.gov.uk

Summary: Intervention and Options

RPC Opinion: Fit for purpose

Cost of Preferred (or more likely) Option (in 2019 prices)			
Total Net Present Social Value	**Business Net Present Value**	**Net cost to business per year**	**Business Impact Target Status**
not quantified	not quantified	not quantified	

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

The next generation 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. The next few years will see increased investment in these networks. 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. That is why DCMS, supported by the National Cyber Security Centre, undertook a comprehensive review of the supply arrangements for telecoms critical national infrastructure. The Review addressed three questions: a) how to incentivise telecoms operators to improve security standards, b) how to address the security challenges posed by vendors, especially those that are high risk, and c) how to create sustainable diversity in the telecoms supply chain. The NCSC security analysis underpinning the Review highlighted a number of key security risks associated with the telecoms supply chain: i) national dependence on any one vendor, especially ones deemed high risk, ii) faults of vulnerabilities in network equipment; iii) embedding malign functionality in vendor equipment; and iv) vendor administrative access to provide equipment support or as part of a managed service contract.

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

To have higher standards and practices of cyber security across the telecoms sector through a new, robust security framework set out in the Telecoms Security Bill. It will do this by strengthening the existing security duty on operators of public electronic communications networks and services with a new overarching duty and sub duties to ensure that telecommunications providers apply appropriate and proportionate measures to prevent, remove or manage the risks to the security of networks and services. It will create a power for the Secretary of State to issue a code of practice. Operators will be able to comply with the security duty with reference to the Code of Practice. The Review was clear that the new telecoms security requirements, at the heart of the telecoms security framework, would be finalised in conjunction with industry, before being enforced under a new legal framework. The initial development of new requirements has been led by NCSC. The NCSC's Telecoms Security Requirements (TSR) are expected to form the technical backbone of the Code of Practice. The NCSC's TSR is a set of principles, requirements and tests that show operators how to protect their network. The intention of the TSR is to create practical controls to 'make it hard for an attacker to compromise a UK network, make it likely that any such compromise will be noticed quickly and the harm and impact limited, and make remediation as simple as possible.'[1]

[1] Summary of the NCSC's security analysis for the UK telecoms sector, 2020, Paragraph 7.1.1.

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

Do nothing: The 'do nothing' option would be to leave the existing framework under the Communications Act 2003 in place. But the Review found that this was not adequate in addressing the threat assessment. The Review recommended that a set of guidance be developed and the NCSC is currently developing this guidance which will initially sit within the current security framework.

Preferred option: To create a new security framework within which the Government sets out what good security looks like with a new security obligation on operators to raise the height of the security bar. Guidance does not provide sufficient incentives for telecoms operators to internalise the costs and benefits of security. The Telecoms Security Bill will create the framework via a set of duties and sub duties; secondary legislation will set out a longer set of security requirements setting out actions that must be taken to achieve the security outcomes; a Code of Practice will set out how operators can meet that framework. Government will consult on the Code including options for its implementation such as the scope of application; how the Code will be used by Ofcom and timescales for implementation.

Does implementation go beyond minimum EU requirements?		N/a			
Is this measure likely to impact on international trade and investment?		Yes			
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes	
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** N/A		**Non-traded:** N/A	

Will the policy be reviewed? A Post Implementation Review of the proposed powers will take place at the latest by 01/01/2026. **If applicable, set review date:** 01/01/2026

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 : Catherine Colebrook Date: 5 June 2020

Summary: Analysis & Evidence

Policy Option 1

Description: The Telecoms Security Bill will set out a new set of duties on operators to make clear the security outcomes we expect that they adhere to. To help operators to achieve these outcomes, the DCMS Secretary of State will be given delegated powers to make secondary legislation containing more detailed sub-duties and requirements, and the power to publish a Code of Practice (or multiple Codes of Practice for different groups of operators).

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	**PV Base** Year 2020	**Time Period** Years	**Net Benefit (Present Value (PV)) (£m)**		
			Low: Optional	**High: Optional**	**Best Estimate:**

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

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

We have not been able to estimate costs to operators as a result of the Telecoms Security legislation. Whilst we had planned a questionnaire to gather cost information; this was cancelled to reduce the burden on telecoms operators responding to the Covid-19 crisis as critical national infrastructure. DCMS intends to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

We understand that the largest operators could incur potentially significant costs but that there is currently a large degree of uncertainty on the level of those costs.The costs that other operators will incur is dependent on how the proposed Code of Practice is implemented for non Tier 1 operators.

Whilst we have not been able to carry out a structured assessment of costs to operators, feedback from bilateral discussions with Tier 1 operators have indicated that the costs of implementing the NCSC TSR would be significant. The scale of these costs is likely to differ by size of operator and could be of the scale of over £10 million in one off costs and the same magnitude of ongoing costs (over the impact assessment period) for an approximately median sized operator.

We have estimated familiarisation and oversight costs but these are likely to be a small proportion of total costs. We have therefore not provided a best estimate of total costs. The estimates of familiarisation and oversight costs are set out below:

- Familiarisation costs: we estimate that they could total a one-off cost of £0.1-£0.2m for 10-20 Tier 1 operators and £1-2m for all other non Tier 1 operators.
- Oversight and enforcement costs: we estimate these costs will be a total cost of circa £30-50m.

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

- Assurance costs: Companies will be required to provide Ofcom with information that sets out how they comply with their overarching security duty set out in primary legislation, having reference to their compliance to any Code of Practice issued by the Secretary of State.

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'

Unlocking 5G use cases: We have estimated the economic impact of 5G use cases that rely heavily on networks that are highly secure and reliable. The Telecoms Security legislation will raise the level of security within networks; we make the assumption that the TSR will contribute to unlocking those use cases as the improved level of security in the network will encourage their rollout and take up where they would not have been deployed otherwise.

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 Telecoms Security legislation. We do not have any information on which to base such an assumption.

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

- Security incidents such as data breaches and cyber attacks, whether intentional or unintentional, can cause significant network disruption and cost to telecoms operators. The Telecoms Security legislation will help harden the network against attack and reduce security risks by reducing the impact of a cyber attack or network outage

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

We have not been able to estimate costs to operators as a result of the Telecoms Security legislation. Whilst we had planned a questionnaire to gather cost information; this was cancelled to reduce the burden on telecoms operators responding to the Covid-19 crisis as critical national infrastructure.

It is also the case that:

- The 'business as usual' scenario is evolving: NCSC have not yet published their guidance and we don't know to what degree operators will implement the guidance once it is published.
- There is uncertainty about what the Government's Code of Practice will look like and we don't know how operators will implement the Code of Practice once it is in place. Also, we have not yet set implementation timescales for the Code of Practice and this is likely to be a key driver of costs.

DCMS intends to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

BUSINESS ASSESSMENT (Option 1)

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

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. The concerns that triggered the review 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.'[2] 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 (TSR).
- Establishing an enhanced legislative framework for security in telecoms
- Managing the security risks posed by vendors.

1.4. This impact assessment accompanies the Telecoms Security Bill and in particular the legislation which aims to create an 'enhanced legislative framework for security in telecoms' - the Telecoms Security Legislation. A separate impact assessment considers the national security powers in relation to high risk vendors which address the need to manage the security risks posed by vendors and are also part of the Telecoms Security Bill.

5G and full fibre networks must be secure and resilient

1.5. The deployment of 5G and full fibre networks across the UK is a primary objective of Government policy. The Government ambition is to deliver nationwide coverage of gigabit capable networks as soon as possible. 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.

1.6. 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. 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.

1.7. These are set out in Box 1 which is an extract from the Review[3]:

[2] The Review, paragraph 1.3.

[3] 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 operators will tend to use their current 4G vendors for 5G rollout.

1.8. Likewise, increasing reliance on FTTP will make the security and resilience of these networks important.

1.9. This is explained in Box 2 which is an extract from the Review[4]:

[4] 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, operators 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 operators in the event of a significant and sustained network disruption, switching between FTTP networks will require engineer visits and new customer premise equipment.

1.10. In conjunction with these technological changes, increasing reliance on telecoms networks for our daily lives is changing the degree to which we rely on 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.

1.11. 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. In exceptional scenarios the criticality of telecommunications networks could be heightened. For example, the Covid-19 pandemic has demonstrated the need for new FTTP networks to be secure and resilient to support national economic activity.

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

1.12. 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.'[5]

1.13. The second and third of these factors relate to market failures that may prevent economically efficient decisions being made from a societal point of view. These are:

- *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 operators 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

[5] 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.

security compared to other factors such as cost and quality[6]. The same is true of businesses: the Cyber Breach Survey 2020[7] found that only 15% of all businesses surveyed have reviewed the cyber security risks presented by their suppliers.

1.14. 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 are the current or future harms being tackled?

1.15. The NCSC provided the expert technical cyber security analysis to inform the Review. This considered the threats and risks to the UK telecoms sector.

1.16. The Review set out a telecoms sector threat assessment. The non-classified element of this assessment is reproduced in Box 3 below which is an extract from the Review[8]:

Box 3: Telecoms sector threat assessment

The most significant cyber threat to the UK telecoms sector comes from states. The UK Government has publicly attributed malicious cyber activity against the UK to Russia and China as well as North Korea and Iranian actors – and each have intentionally inflicted damage on the UK through cyber means.

For example, in December 2018 the UK along with its Allies announced that a group known as APT10 acted on behalf of the Chinese Ministry of State Security to carry out a malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the US.

Additionally, in November 2017 the NCSC publicly stated that they had seen evidence of Russian attacks against UK telecoms networks. The targeted networks did not contain Russian equipment, but were affected by architectural weaknesses that the attackers were able to exploit.

Actors may seek to exploit weaknesses in telecoms service equipment, network architecture and/ or operator operational practices, in order to compromise security. The weaknesses could result from design defects, whether voluntary or not, configuration errors in the deployment of equipment by operators, or illegitimate actions by individuals working for vendors or operators in the maintenance and administration of such equipment.

[6] 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.

[7] 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.

[8] The Review, paragraphs 3.2 - 3.8.

Some states have significant access to the telecoms sector supply chain, principally through a domestic business supplying equipment and other services, and through foreign direct investment. These activities might negate the need to mount operations (cyber or otherwise) to deliver limited compromise of telecoms networks. As well as espionage, states may seek to conduct disruptive or destructive operations under certain circumstances.

As set out in the previous section, the move to 5G brings a new dimension to the security risks, given the greater dependence that wider UK CNI is likely to have on UK telecoms than is the case with 3G/4G. The NCSC concludes that if new 5G use-cases emerge at scale, a successful cyber attack could be highly disruptive across UK CNI and the wider economy.

Based on experience from security testing[9] and security incidents, the NCSC assesses that existing vendor agnostic security mitigations, as applied across the telecoms sector, are at best only moderately effective. While this evidence is by no means comprehensive, it points to a telecoms sector that needs to improve cyber security practices. In addition, 90% of the significant security incidents reported to Ofcom in 2018 are attributed to system failure (including hardware or software failures, and systems, processes and procedures failures).[10]

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

1.18. Findings from the UK Cyber Breaches Survey 2020[11] 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.

1.19. 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.

[9] The National Cyber Security Programme funded intelligence-led penetration testing pilots (TBEST) highlighted a number of cyber security vulnerabilities. The companies have remediation plans to address and mitigate those vulnerabilities. Responsibility for the rollout of TBEST has now passed to Ofcom.

[10] *Connected Nations 2018*, Ofcom, December 2018 https://www.ofcom.org.uk/research-and-data/multisector-research/infrastructure-research/connected-nations-2018/main-report

[11] Cyber Security Breaches Survey 2020: Statistical Release

What sectors/markets/stakeholders will be affected?

1.20. 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).[12]

1.21. Sections 105A-D (security of public electronic communications networks and services) Communications Act 2003 provides the current legislative framework for telecoms security, overseen by Ofcom. It provides that all telecoms operators must take technical and organisational measures to appropriately manage security risks. New legislation will look to enhance this framework, to level up security across the industry.

1.22. Ofcom has published guidance to assist telecoms operators (ie PECN and PECS) in complying with their current obligations under the Communications Act. In issuing this guidance Ofcom is "encouraging compliance by explaining the security and resilience (statutory) obligations imposed on relevant communications providers, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns."

1.23. The guidance sets out that it is "for communications providers themselves to determine how their statutory obligations affect their activities and take any necessary measures in order to comply with them." Ofcom oversees and enforces compliance with s105A *ex post* through monitoring reports of breaches and auditing a network or service providers security measures where necessary as well as enforcement.

1.24. The scope of the Review was also PECS and PECN, which shaped the engagement and policy recommendations made in the Report - including the establishing the need for a new, robust security framework. Reflecting this, the Telecoms Security Bill is expected to apply to PECN/PECS as defined in the Communications Act.[13]

1.25. The security duties in primary legislation will apply universally to all public telecoms providers - that is because irrespective of size it is vital that the public have confidence and assurance that their communications are secure. However, in recognition that the detail of the security expectations should be proportionate to the size of the operator (reflecting the different scale of the impact that any security breach of potential loss of services is likely to have) the detailed measures that will set out how best to comply with the duties will be tailored through the Codes of Practice. The Codes of Practice will distinguish between what measures are expected of different-sized operators through a tiering system - Tier 1 for the largest operators, Tier 2 for medium sized operators, or operators

[12] 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". Electronic communications service: "any electronic communications service that is provided so as to be available for use by members of the public".

[13] It should not directly apply to equipment vendors or managed service providers, though these entities will be impacted indirectly. Operators who provide bespoke private networks to business customers would not be included in this definition.

forming critical national infrastructure, and Tier 3 for all other operators. An initial Code of Practice is expected to be applied to the Tier 1 scale operators who serve the majority of the retail and business markets and whose network security is of critical importance to the UK. It is also expected to apply to Tier 2 medium-sized operators whose security is critical to regional availability, with a lighter approach to assurance oversight by Ofcom and longer timetables for implementation

1.26. In addition to new duties placed on operators, Ofcom will be impacted through resource requirements to carry out enhanced reporting and oversight duties. The Department for Digital, Culture, Media and Sport (DCMS) will also be affected through new responsibilities and functions - such as issuing Codes of Practice - that are placed on them.

Why is the government best placed to resolve the issue?

1.27. 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 assessing risks and taking appropriate measures to ensure the security and resilience of their networks.

1.28. 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.

1.29. 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. And that, therefore, the role of policy and regulation in defining and enforcing telecoms cyber security needs to be significantly strengthened to address these issues.

2. Rationale and evidence to justify the level of analysis

The Telecoms Supply Chain Review

2.1. 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.

2.2. The Review engaged extensively with the UK telecoms industry, including telecommunications providers and equipment suppliers, whilst respecting the need to protect highly sensitive commercial and security information.

2.3. Officials carrying out the Review wrote to the major telecoms operators[14] and suppliers[15] informing them of the Review and inviting them to contribute. They held meetings with operators, issued a questionnaire, and collected extensive amounts of information from them under a series of non-disclosure agreements. In addition, they met and gathered information from trade associations, industry bodies and international standards organisations (including GSMA[16], ETSI[17] and 3GPP[18]).

2.4. The engagement with operators and vendors centred around two sets of questions developed in conjunction with NCSC: one for network operators and one for equipment vendors. Those questions formed the basis of an information request sent out to 20 companies / entities that are active in the UK. In most cases, the companies met face-to-face to discuss the questions and how best to answer them.

2.5. The telecoms industry engaged positively with the Review and most of the companies that were approached provided contributions. The information provided by industry totalled nearly 700 pages, not including additional material sent directly to NCSC.

2.6. DCMS published the Review Report in July 2019 setting out the key proposals for a new telecoms security framework. This would be centred on new Telecoms Security Requirements (TSR) - published as guidance by the NCSC in the first instance - to indicate to industry what good security looked like. It would be underpinned by an enhanced legal framework under new legislation.

Assessing impacts and ensuring proportionality

2.7. The Review was clear that the new Telecoms Security Requirements at the heart of the telecoms security framework would be finalised in conjunction with industry,

[14] BT, Openreach, EE; Cityfibre; Gigaclear; Hyperoptic; KCOM; MBNL; O2 (Telefonica); Sky; TalkTalk; Three (3); Virgin; Vodafone; and Linx.

[15] Cisco, Ericsson, Huawei, Nokia, Samsung, and ZTE.

[16] The GSMA is an industry organisation that represents the interests of mobile network operators worldwide.

[17] Electronic Telecommunications Standards Institute

[18] The 3rd Generation Partnership Project is an umbrella project for a number of telecommunications standards development organisations (including ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

before being enforced under a new legal framework. The Review set out these would need to be targeted, proportionate and actionable.

2.8. The initial development of new telecoms security requirements has been led by NCSC - it is part of NCSC's role to highlight potential cyber security risks to the UK's national security and provide advice based on technical expertise. NCSC issued a draft of the requirements to large telecoms operators for comment and input in December 2019, via its Network Security Information Exchange forum[19]. The guidance will form the basis for technical security measures under a future legal framework. This was initially expected to be finalised and issued in Spring 2020 but the purdah restrictions around the general election and the more recent Covid-19 pressure on operator resourcing has made industry engagement challenging.

2.9. This NCSC-led engagement was to allow industry input on the technical workability of the measures. The detail of the measures have been changing based on operator feedback. These continued NCSC-led discussions with industry on the details of technical security measures have meant it has not yet been possible to formally consult industry on implementation. Technical details to mitigate risks must be agreed before industry is able to assess costs and before a proportionate implementation approach can be consulted on.

2.10. DCMS did attempt to obtain information on the scale of costs to the NCSC guidance as it stands to provide an indication of the potential costs of the Telecoms Security Legislation. DCMS did this by engaging with larger operators who have been involved in workshops with NCSC on finalising technical details. Collectively these large industry players cover the majority of the FTTP and 5G industry, making up over 85% of the mobile network operators and over 85% of the fixed operators (by market share). We issued a survey to these operators on 11 March 2020. Whilst this survey was directed to a limited number of operators, we hoped to use the output on familiarisation costs and costs as a proportion of turnover to estimate the potential scale of impact on other operators.

2.11. The survey was a structured set of circa. 50 questions asking operators for information on the degree to which they currently comply with the NCSC's guidance and the ongoing and one-off costs of implementation. The survey covered costs of each area of the guidance including:

- management plane
- signalling plane
- virtualisation plane
- supply chain
- loss of national capability to operate UK networks.

2.12. It also included details of overarching costs including supporting business processes and security audit and investigation.

2.13. However, the Covid-19 crisis placed severe strain on operators' availability to input to this survey. Technical and operational leads working with NCSC on development of guidance were required to prioritise company responses to

[19] This voluntary information sharing forum consists of 20 members who represent the UK's major fixed and mobile network providers for both business-to-consumer and business-to-business markets.

changing connectivity demands as a result of the crisis. Those Covid-19 responses have been coordinated across the telecoms sector by DCMS and operators have been taking exceptional measures to ensure the UK's networks can cope with new demand patterns. This unavoidable conflict led operators to request that DCMS withdraw the survey, which we did after establishing that operators were not able to complete even an amended and simplified version.[20]

2.14. Without this survey we will have limited information on the direct costs to business of the NCSC guidance. However, bilateral feedback that we have had indicates that: because the NCSC guidance is currently in draft form there are a wide range of possible costs depending on the outcome of the final draft; and operators do not yet have estimates of the costs of implementation because they are still familiarising themselves with the guidance.

2.15. We are also aware that the legal status of the different parts of the new security framework - including the final form of technical guidance issued by the NCSC and its relationship to Ofcom's enforcement of operator duties under the new framework - will be key to assessing the impact on affected companies. Detail on this is set out below.

2.16. DCMS intends to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

What will legislation seek to do?

2.17. The Telecoms Security Bill once enacted will implement some of the proposals of the Supply Chain Review. We intend the legislation to:

- Provide new legal security duties for providers of electronic communications networks and services (PECN/PECS as defined in the Communications Act) to ensure adequate security of networks;
- Provide a new duty for Ofcom to promote the security and resilience of PECN/PECS, to enhance its existing powers in this area;
- Provide a delegated power to make secondary legislation setting out sub-duties and detailed security requirements to further define the priority actions to be taken by PECN/PECS; and
- Provide powers for the DCMS Secretary of State to set out new Security Codes of Practice to assist Ofcom and relevant PECN/PECS on how they might meet their new duties,sub-duties and requirements.

2.18. Alongside this legislation, the Government is also proposing to introduce through the other part of the Telecoms Security Bill 'the national security powers relating to high risk vendors' which seek to implement further proposals from the Supply Chain Review. Those powers will seek to limit the use of equipment provided by high risk vendors in UK telecommunications networks. They provide the Secretary of State with the ability to designate vendors as high risk; issue directions to telecoms operators placing controls on the use of equipment from high risk vendors; and require operators to provide information to the Secretary of

[20] DCMS received one response to the survey.

State on existing and planned vendor arrangements and wider network details to enable the Secretary of State to effectively apply and assess compliance with the controls. Those proposals are considered in a separate impact assessment.

How will the legislation work?

2.19. The duties and sub-duties will apply to all PECN/PECS, will be limited in number, be general enough to be applicable in some form to all, and easily understood by any affected parties.

2.20. The Bill will contain **an 'overarching' security duty** for all providers of public electronic communications networks or services to take appropriate security measures to address risks to the security of networks and services of all kinds (and including reducing impacts of security incidents and incident recovery).

2.21. Secondary legislation will then set out 5-10 more specific **security sub-duties** detailing the security outcomes that providers need to achieve and a longer (between 40-50) set of **security requirements** setting out actions that must be taken to achieve the security outcomes;

2.22. **Finally, there will be detailed and specific security measures** for certain types of provider, set out in codes of practice, that demonstrate how those providers are expected to comply with their legal obligations.

2.23. The codes of practice are the way in which DCMS seeks to demonstrate what good security practices look like in the context of the new duties, and the way that we ensure the security framework is targeted, proportionate and actionable. The scope of application will be set out within the Codes themselves. The contents of the Code to be applied to Tier 1 larger operators will use the NCSC guidance as its technical backbone for large operators.

2.24. To provide clarity to industry and Ofcom on the new framework, primary legislation will set out the need for relevant PECN/PECS to have due regard to relevant Codes. As any Codes will not be statutory there will be discretion for operators as to whether they seek to meet their legal duties in other ways that they believe are more proportionate and appropriate to their business and network operations. In any event, operators will be expected to set out to Ofcom how they meet their legal obligations. By taking this approach we are seeking to implement a more proportionate set of requirements that will prevent unnecessary costs to business.

2.25. To ensure complete clarity on the relationship between any Code and input to compliance with legal duties, Ofcom will be provided with the power to issue procedural guidance on its assessments against the legal duties.

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

2.26. New legal duties and sub-duties will represent an absolute minimum for what is required to ensure network security is adequate and risks to national networks are mitigated. Operators may seek to meet those in various ways but DCMS recognises that many operators may choose to follow the detail set out in a Code of Practice as targeted, actionable measures.

2.27. 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.

2.28. DCMS intends to open a public consultation subsequent to the passage of secondary legislation, on the relevant aspects of an initial Code of Practice for larger operators. However, DCMS will engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

2.29. A consultation at that point would be expected to set out:

- The scope of application of the Code;
- How the Code could be used for the purposes of compliance with Ofcom enforcement of legal duties;
- Implementation of the new legal duties and proposed timescales for compliance.

2.30. Only once a full public consultation had concluded and responses fully evaluated the position of a Code in the new legal framework would be finalised and published.

3. Description of options considered

The 'Do nothing option' or 'Business as Usual'

3.1. Business As Usual, or the status quo is the continuation of current arrangements as if the intervention under consideration were not to be implemented. This is termed the 'do nothing' option' and in this case refers to continuing with the existing security requirements under the Communications Act 2003.

3.2. We discussed in section 1 the Problem under consideration and rationale for intervention. As 5G and full fibre technology is rolled out we explained that the security requirements are changing and that this creates a need for a new security framework. The 'do nothing' option would be to leave the existing framework under the Communications Act 2003 in place. But 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.'[21]

3.3. In addition to the requirements contained in the Communications Act, NCSC is producing a set of guidance to provide operators with a baseline of security controls to protect operator networks from realistic and nationally significant cyber attacks . This guidance is non-binding but the Review set out how this guidance would be implemented within the current regulatory framework. It stated that Ofcom should:

- Include the finalised TSR, where appropriate, in its industry guidance, and use that to engage industry to understand supply chain risks and the arrangements adopted by operators to mitigate them;
- Engage industry as part of its Security and Resilience Assurance Scheme to gain regular updates on operators' major supplier arrangements and TSR compliance plans, including how they are being dealt with at Board level;
- Where there is reason to suspect that conduct may also be a breach of a provider's security and resilience obligations, use its current information gathering and audit powers to investigate suspected breaches of the TSR;

[21] 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.

- Encourage providers to participate in Ofcom's threat intelligence-led penetration testing scheme (TBEST) and, subject to third party contract arrangements, test operators' vendor specific arrangements. Subject to any applicable restrictions on the disclosure of information, Ofcom would also aim to share thematic findings across the sector to support a culture of continuous improvement; and
- Increase analysis and reporting on network security and resilience.[22]

The Preferred Option

3.4. In this impact assessment we only consider one option - to create the Telecoms Security legislation including the overarching duty and sub- duties - these duties are set out in section Summary and preferred option.

3.5. However, to help operators to achieve these outcomes, the DCMS Secretary of State will be given the power to publish a Code of Practice (or multiple Codes of Practice for different groups of operators). Government plans to consult on the Code of Practice at the stage of its development.

3.6. During this consultation the Government will consider options that relate to how the Code will be implemented. These could include:

- The scope of application of the Code[23];
- How the Code could be used for the purposes of compliance with Ofcom enforcement of legal duties;
- Implementation of the new legal duties; and
- Proposed timescales for implementation.

3.7. These options could have an important impact on the way in which the Code affects operators. For example, the amount of time within which operators are expected to implement the recommendations in the Code is likely to have an impact on implementation costs.

[22] The Review, Paragraph 5.10.

[23] An initial detailed Code based on NCSC guidance is expected to be applied to a select group of large operators who own and operate critical national networks, and who have been engaged in the drafting of technical detail via NCSC workshops. Subsequent Codes may set out good security practices that are less detailed and more appropriate for smaller operators.

4. Policy objectives

4.1. The purpose of the Telecoms Security Requirements was set out in the Review and is ‘to ensure providers of PECNs or PECSs take appropriate and proportionate measures to prevent, remove or manage the risks posed to the security of networks and services, specifically to ensure:

- that networks and services are accessible and available to customers;
- the confidentiality of communications and data;
- the integrity and authenticity of networks, systems, communications, and sent, received or stored data; and
- the protection of networks and services from unauthorised access or interference.’[24]

4.2. The Telecoms Security legislation will implement the proposals of the Review. With regard to the new security framework, it is intended to:

- Provide new legal security duties for providers of electronic communications networks and services (PECN/PECS as defined in the Communications Act) to ensure adequate security of networks;
- Provide a new duty for Ofcom to promote the security and resilience of PECN/PECS, to enhance its existing powers in this area;
- Provide a delegated power to make secondary legislation setting out sub-duties and detailed security requirements to further define the priority actions to be taken by PECN/PECS; and,
- Provide powers for the DCMS Secretary of State to set out new Security Codes of Practice to assist Ofcom and relevant PECN/PECS on how they might meet their new duties,sub-duties and requirements.

4.3. The duties,sub-duties and requirements for all PECN/PECS will be general enough to be applicable in some form to all, and easily understood by any affected parties.

4.4. The Codes of Practice are the way in which DCMS seeks to demonstrate what good security practices look like in the context of the new duties, and the way that we ensure the security framework is targeted, proportionate and actionable. The scope of application will be set out within the Codes themselves. The contents of the initial Code are likely to closely resemble the NCSC’s draft Telecoms Security Requirements for large operators.

[24] The Review, Page 36.

5. Preferred option with description of implementation plan

5.1. The Telecoms Supply Chain Review published in July 2019 set out the need for a stronger regulatory framework for telecoms security.

5.2. Based on the recommendations of that review the Telecoms Security legislation should act to “raise the bar” for security within the telecoms sector, and in particular within the most significant telecoms operators such as BT and Vodafone.

5.3. The legislation will set out:

- **An 'overarching' security duty** in the Bill for all providers of public electronic communications networks or services to take appropriate security measures to address risks to the security of networks and services of all kinds (and including reducing impacts of security incidents and incident recovery); and
- A set of 5-10 more specific **security sub-duties**, set out in secondary legislation, detailing the security outcomes that providers need to achieve.
- A longer (between 30-50) set of **security requirements,** also in secondary legislation, setting out the actions that must be taken to achieve the security outcomes.

5.4. We do not expect that the overarching security duty in the Bill alone would have a significant impact on those companies subject to it. This is because these duties are a breakdown of what we might already expect operators to be doing to meet their existing obligation at S105A of the Communications Act 2003. The key elements of the duties will require PECN and PECS to identify, manage, reduce and facilitate recovery from security risks to networks. An operator complying with the existing requirements in the Communications Act would be likely to need to carry out similar activities.

5.5. So while the primary duties may be more detailed than existing requirements, we anticipate that it is the specific sub-duties and security requirements that will be set out in secondary legislation that will determine the level of impact on operators. The impact of these sub-duties and requirements will be assessed in the impact assessment accompanying secondary legislation.

5.6. To help operators to achieve these outcomes, the DCMS Secretary of State will be given the power to publish a Code of Practice (or multiple Codes of Practice for different groups of operators).

5.7. Communications providers must demonstrate to Ofcom how they comply with these duties. In carrying out these measures and demonstrating compliance, relevant communications providers must have due regard to managing the priority risks to networks and services as set out by the Secretary of State in any applicable Codes of Practice.

5.8. Key to this framework is that the Code of Practice will set out baseline expectations of how the high level security duties can be achieved. This will give operators clear guidance on how to achieve their legal duties, but still allow flexibility for operators with different network setups.

5.9. We are proposing a tiered approach to the Codes of Practice, where larger operators were expected to take a greater level of measures (which will largely mirror those set out in the current NCSC draft TSR) smaller operators will have to follow a subset of these measures. This detail would be set out in the Codes of Practice. This would provide very clear signalling to all operators on the expected level of security.

5.10. Ofcom will be given an expanded security duty to regulate this system, taking regard of the Code of Practice in their regulatory work. This will broadly be using a self-reporting mechanism - operators 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 operators is accurate. We believe that this is a more proportionate approach than a continuous audit model, that would require significant resources from both operators and Ofcom to maintain.

5.11. 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. The current appeals system will also be utilised.

5.12. Following consultation, the Codes of Practice will set out the implementation expectations. A mixed approach will be necessary and proportionate to reflect the fact that operators will have different levels of existing compliance with the new framework given their existing security obligations.

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

Limitations of the calculations and estimates

6.1. This impact assessment does not estimate the costs of the proposed policy option except in the case of familiarisation costs and monitoring costs. 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 analysis.

- NCSC have not yet published their TSR which is expected to form the technical backbone of the Code of Practice.
- We don't know to what degree operators will implement the NCSC's TSR as non-binding guidance. Knowing what good looks like could have a powerful effect. It will provide regulatory certainty for operators who will know what is expected of them in clear terms. It will mean that changes to relationships with suppliers take place on a level playing field with all operators requiring the same changes. It will facilitate collaboration on how to implement the guidance across industry creating knowledge sharing benefits.
- We don't know what the Code of Practice will include and how operators will implement the Code of Practice once it is in place.
- We have not yet set implementation timescales for the Code of Practice and these are likely to be a key driver of costs.

6.2. 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 TSRs to the degree that these costs are related to the size of the network. This includes uncertainty in relation to the number of networks affected. New operators may enter the market as 5G and full fibre networks grow and we cannot know how the TSR will affect these networks now.

6.3. 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.

The costs and benefits of the proposed approach

6.4. The preferred policy option set out in the section Summary and preferred option with description of implementation plan is to legislate for a new overarching security duty in the Bill, followed by secondary legislation setting out sub-duties and requirements on operators to make clear the security outcomes that they must adhere to. To help operators to achieve these outcomes, the DCMS Secretary of State will be given the power to publish a Code of Practice (or multiple codes of practice for different groups of operators).

6.5. For the purposes of this impact assessment we have not been able to estimate the direct costs to industry of implementing the new set of duties and requirements or the Code of Practice directly; by which we mean using data provided by industry. We explain this in the section above on Rationale and evidence to justify the level of analysis used in the IA (proportionality approach).

6.6. DCMS intends to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

6.7. For the purpose of this Impact Assessment, we are not able to provide an estimate of total costs or net costs to business per year. However, we have set out to describe the types of costs that will be incurred below.

What is the counterfactual

6.8. In the section Description of options considered we set out the 'do nothing' option which is also our counterfactual. This is:

- Continuing with the existing security requirements under the Communications Act 2003. Taking into account the forthcoming NCSC Telecoms Security Requirements guidance. The guidance is expected to provide clarity on the cyber standards and practices that are expected of industry and reduce the complexity of delivering, monitoring and enforcing contractual arrangements in relation to security.

6.9. The NCSC's TSR was created as a result of the Review which recommended that the TSR be created and, later, be put on a statutory footing. This Impact Assessment is concerned with creating the statutory duties and sub duties on operators to make clear the security outcomes we expect that they adhere to.

6.10. As a result the appropriate counterfactual is that we continue to rely on the existing security requirements with the addition of NCSC's TSR with the status of guidance. In this case industry would be likely to accrue some costs - and also some benefits - of improving security. The degree to which they do this will affect both the costs and the benefits that will result from the Telecoms Security legislation

Economic impact - costs

6.11. 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 and type of businesses that will be affected

6.12. The scope of the Review was PECS and PECN - this shaped the engagement and the policy recommendations made in the review - including the recommendation that the telecoms security requirements be created.

6.13. Reflecting the Review, at a high level the Telecoms Security Legislation should apply to providers of electronic communications networks[25] or services[26] (PECN/PECS) as defined in the Communications Act.[27]

6.14. The security duties in the Telecoms Security Bill and the detailed requirements to be set out in secondary legislation will apply universally to all telecoms operators - that is because irrespective of size it is vital that the public have confidence and assurance that their communications are secure. However in recognition that the detail of the security expectations should be proportionate to the size of the operator (reflecting the different scale of the impact that any security breach of potential loss of services is likely to have) the detailed security measures that will set out how best to comply with the duties and requirements will be tailored through the Codes of Practice. There will be three Codes of Practice - Tier 1 for the largest operators, Tier 2 for medium sized operators, or operators forming critical national infrastructure, and Tier 3 for all other operators.

6.15. The operators in Tier 1 could change over time. In the first instance we expect it would include scale operators who serve the majority of the retail and business markets and whose network security is of critical importance to the UK. These operators are already engaged with the NCSC and Ofcom on improving network security.

6.16. For the purpose of this impact assessment we estimate that there will be between 10 and 20 Tier 1 operators.

6.17. The total number of PECN/PECS, who make up Tiers 2 and 3, is much greater. We set out available information on the number of PECN and PECS below.

6.18. Available information shows that:

- There were 119 PECS and PECN who paid Administrative fees to Ofcom and therefore have a turnover of over £5m in 2019/20[28]
- There were 228 PECN and PECS who had 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' on 3rd March 2020.[29]

[25] A 'public electronic communications network' is defined in section 151 of the Communications Act 2003 as: "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public".

[26] A 'public electronic communications service' is defined in section 151 of the Communications Act 2003 as: "any electronic communications service that is provided so as to be available for use by members of the public".

[27] An 'electronic communications network' is defined in section 32 of the Communications Act as:

- a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and
- such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals—
- apparatus comprised in the system;
- apparatus used for the switching or routing of the signals;
- software and stored data; and
- (except for the purposes of sections 125 to 127) other resources, including network elements which are not active."

[28] Operators who have paid Administrative fees to Ofcom under section 38 of the CA 2003 in 2019/2020 and therefore had a turnover of over £5m in 2017. There are 119 such companies. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/101899/network-service-providers-admin-charges.pdf

[29] Operators 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', 3rd March 2020.

6.19. These two categories are likely to overlap as operators that pay Administrative fees may also have applied for Code powers.

6.20. In addition to these companies, there may be further PECN/PECS who have a relevant turnover of under £5m and do not have Code powers. We refer to these companies as the 'long tail'. As a reference point we note that there are approximately 8,000 micro and small businesses reported by the ONS in industry classification code 61 (telecommunications).

6.21. The Telecoms Security legislation will not directly apply to equipment vendors or managed service providers, though these entities will be impacted indirectly. We do not estimate costs for these companies as these costs will be ultimately paid by PECS and PECN who use the services that these companies provide.

Familiarisation costs

6.22. There will likely be significant familiarisation costs as operators get ready to embed the Telecoms Security legislation into their business processes. These costs include understanding the legal duties and reading and understanding the relevant Code of Practice.

6.23. As the Code of Practice has not yet been drafted we cannot estimate familiarisation costs associated with it. As a proxy we therefore consider the familiarisation costs associated with the NCSC's TSR, which are expected to form the technical backbone for any future Code of Practice and therefore is a suitable proxy for the Code.

6.24. We note that operators may incur familiarisation costs twice;

- first in reading and understanding the NCSC's TSR; and
- then in reading and understanding the legal duties and Code of Practice.

6.25. In addition we note that the Government's clear intention to legislate means that operators may incur more familiarisation costs in reading and understanding the NCSC's TSR than they would otherwise have done i.e. they may not wait for the Code of Practice but seek to familiarise themselves early.

6.26. We have therefore taken a pragmatic approach to providing an estimate of the scale of familiarisation costs with reference to what we know about the costs operators have incurred in familiarising themselves with the NCSC's TSR so far.

6.27. The NCSC's TSR is a lengthy document containing 13 sections each of which includes principles, requirements and tests. We have estimated the costs of reading and understanding the guidance by a member(s) of an organisation's security team. We recognise that operators 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 TSR more widely to staff in order to embed new processes into their business.

6.28. The NCSC first issued a draft version of the TSR on 6 December which was shared with larger operators. These operators have input to an engagement process with NCSC whereby they have reviewed the draft TSR in detail. For

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 example, we are aware that these operators have attended a number of workshops to this effect.

6.29. The costs that these operators have incurred provide an indication of the potential familiarisation costs that other operators will incur in familiarising with the Telecoms Security Legislation. Although we expect that these operators would incur higher costs because they have familiarised themselves with draft versions of the guidance and provided input on those drafts.

6.30. Based on bilateral discussions with Tier 1 operators and considering the number of requirements contained in the NCSC's guidance we estimate that familiarisation costs could include at least 200 hours from a member of an organisations security team for a Tier 1 operator on average. There will be further one-off costs as operators disseminate the TSR across other areas of their organisation and begin to design processes around it.

6.31. We expect non tier 1 operators will incur lower costs due the potential mitigation of the scope of the Code for these operators and a lower absolute impact on operators of smaller size. We therefore estimate that all PECN/ PECS that have applied for Code powers incur half of this amount i.e. 100 hours.

6.32. We do not estimate any familiarisation costs for the long tail of PECN and PECS. Whilst some operators in the long tail may familiarise themselves with the NCSC's Telecoms Security Requirements or the Code of Practice when it is implemented, it is equally possible that they will not. We also note that there is inherent uncertainty about the number of PECN and PECS there are in the long tail and that Ofcom does not currently actively engage these operators.

6.33. By way of illustration; if the long tail is twice the size of the number of PECS/ PECN with Code powers but these operators incur half the familiarisation costs on average we estimate they will incur the same level of familiarisation costs as the PECN and PECS category.

6.34. Further work is needed to understand the impact of familiarisation costs on operators. This would include refining our estimates of the costs of reading and understanding the Code of Practice, considering requirements for legal professionals to understand the statutory duties and considering the costs of disseminating the details of the Code to other staff.

Estimating familiarisation costs

6.35. The wages for information technology and telecommunications directors are taken from the ONS' Annual Survey of Hours and Earnings[30]. The median is used as a best estimate, as it is believed to be the most representative wage (it's less skewed by outliers).

[30] ONS, Annual Survey of Hours and Earnings, Provisional - 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	Uplift for overheads
Job Title	Median			
Tier 1 Operators				
IT specialist managers	36.55	200	£7,310	£8,918
PECN and PECS with Code Powers				
IT specialist managers	36.55	100	£3,655	£4,459

6.36. Overhead charges of 22% are added to the wages, in accordance with RPC guidance on implementation costs[31] which uses Eurostat data on UK non-wage and wage costs to calculate this uplift. the International Standard Cost Model Manual.

6.37. Based on this data familiarisation costs will be:

- At least £9,000 per Tier 1 operator. For 10-20 Tier 1 operators this would total circa £0.1-£0.2m.
- Around £4,000 per PECN/PECS with code powers. Based on 213[32] such operators, this would total around £1m.
- If operators in the long tail incur around £2,000 each and there are twice as many of these as there are PECN/PECS with Code Powers; they would also incur a total of around £1m.

6.38. The number of hours taken to familiarise with the legislation will vary based on how the Code of Practice is implemented. Furthermore, there is a lack of evidence on how these costs will vary by business size. For micro and small businesses, which have fewer resources to manage the change in the legislation, the proportionate burden is expected to be greater but the absolute number of hours may be lower reflecting the way that the Code is applied for smaller businesses and the size of their network.

One off and Ongoing costs

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

[32] 228 operators with Code Powers minus 15 Tier 1 operators.

6.39. In addition to familiarisation costs it is likely that PECN and PECS will make changes to their networks in order to comply with the Telecoms Security legislation. These changes include:

- Changes that Tier 1 operators (including other operators that are designated in the future) will make in order to comply with the duties set out in the Telecoms Security Legislation.
- Changes that other PECN and PECS, will make in order to comply with the duties set out in the Telecoms Security Legislation.

Costs incurred by Tier 1 operators

6.40. New statutory security duties and sub-duties in the Telecoms Security Bill and subsequent secondary legislation will represent an absolute minimum for what is required to ensure network security is adequate and risks to national networks are mitigated. In meeting these, DCMS recognises that many operators will choose to follow the detail set out in a Code of Practice as targeted, actionable measures.

6.41. DCMS will consult on this Code of Practice once the technical detail of NCSC guidance is finalised and will allow maximum clarity to industry stakeholders on what a new Code will contain. This will mean that industry will have a clear picture of the potential costs associated with following technical measures. A consultation at that point on an initial Code would be expected to set out:

- The scope of application of the Code[33];
- How the Code could be used for the purposes of compliance with Ofcom enforcement of legal duties;
- Implementation of the new legal duties and proposed timescales for compliance.

6.42. These factors, and in particular the implementation timetable, are expected to have a significant impact on the costs to operators of complying with the Telecoms Security legislation.

6.43. We are developing the detail of the Code of Practice and the NCSC guidance is expected to form its technical backbone. For the purpose of this impact assessment we assume that the Code of Practice reflects the NCSC's TSR draft guidance and we describe the impact that this guidance is expected to have on an operators network - or the outcomes it hopes to achieve. However, we noted that each operator will accrue different costs depending on their current network and how they choose to implement the Code.

6.44. Bilateral discussions between DCMS and a number of Tier 1 operators on the NCSC guidance have indicated that it is difficult for operators to estimate the costs of their business now because:

- NCSC guidance is currently in draft form and there are a wide range of possible costs depending on the outcome of the final draft; and

[33] An initial detailed Code based on NCSC guidance is expected to be applied to a select group of large operators who own and/or operate critical national networks, and who have been engaged in the drafting of technical detail via NCSC workshops. Subsequent Codes may set out good security practices that are less detailed and more appropriate for smaller operators.

- operators do not yet have estimates of the costs of implementation because they are still familiarising themselves with the guidance.

6.45. We also note that as any Codes will not be statutory there will be discretion for operators as to whether they seek to meet their legal duties in other ways that they believe are more proportionate and appropriate to their business and network operations[34]. Operators have different network set-ups and different business models that would make a one-size-fits-all set of detailed security measures (as set out in the Codes) inappropriate. It should also be noted that the NCSC's TSR guidance aims to set out recommended security controls at a granular level. It does this with the aim of facilitating consistency across the industry. For this reason, a number of the requirements set out in the guidance and described below, may be existing practice for operators. To understand to what degree the TSR are incremental to current security practices each operator would need to set out the changes they would need to make to their own network.

[34] However, in doing so Ofcom would need to be satisfied that the operator's chosen route still delivers the appropriate security outcome.

The NCSC's TSR

6.46. The NCSC guidance is a set of principles, requirements and tests that show operators how to protect their network. Box 4 below describes the NCSC's guidance.

Box 4 - What are the Telecoms Security Requirements?[35]

Since the initiation of the DCMS Supply Chain Review in September 2018, the NCSC has performed an extensive and detailed analysis of the security of the telecommunications (telecoms) sector.[36]

NCSC used attack tree analysis to identify cyber risks to telecoms networks. (Building attack trees allows a significant number of potential risks to be explored, creating a natural grouping of risks into 'themes' or particular areas of concern.) The analysis broke down the threats into four overarching negative outcomes.

- Espionage - stealing or corrupting data in the network
- Disruption - stopping service on part or all of a network
- Pre-positioning - quietly getting a foothold in the network administrative systems to use later
- National dependence - being dependent on a third party for some critical part of the design, procurement, operation, support or incident management of the UK's networks.[37]

Based on these four classes of attack NCSC have generated a set of ways in which an attack could proceed and then a set of methods an attacker could use to proceed (attack vectors). For each vector the NCSC have identified:

- where it could happen on a network;
- how it could be mitigated (protected against); and
- how you'd make sure the mitigation was working.

The result is that, for each attack vector, there is a description of the risk, a set of principles to guide operators to defend against that risk, a list of expected controls, a 'default' implementation to guide the operator, and ways to monitor those security controls. This is what frames the NCSC's Telecoms Security Requirements.

6.47. The NCSC's TSR are built around mitigating five main areas of significant risk:

- management plane
- signalling plane

[35] https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk

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

[37] ibid, section 3.2.

- virtualisation plane
- supply chain
- loss of national capability to operate UK networks

6.48. We describe each of these areas below as set out in the NCSC Security Analysis for the UK Telecoms Sector and highlight potential areas where operators could incur costs.[38] We have used these five areas as the basis of our cost analysis as they present the biggest risks to the networks. This does not necessarily mean that they are the most costly areas to address. As set out in section Number and type of businesses that will be affected we assume that 10-20 Tier 1 operators will be required to comply with the Telecoms Security legislation taking into account the Tier 1 Code of Practice which details the government's 'recommended' way of complying with legal obligations. Non-tier 1 operators may also incur costs where they need to comply with the Telecoms Security legislation taking into account relevant Codes of Practice.

The management plane

6.49. The management plane of a network is where administrative activity takes place. It is used for provisioning and configuration of new equipment and making changes to existing infrastructure or services amongst other things.

6.50. The NCSC found that 'historic management of telecoms networks' has relied heavily upon standard corporate devices 'doubling up' as administrative workstations. Consequently, the laptops that perform standard 'office' type functionality such as email, web access and productivity tool use are also defining the operation of the network. This can lead to several 'commodity' classes of attack being performed with relative ease on administrative users and these can achieve a significant impact. Attacks of this type may also not always be easily detected, as there may be no overt impact on the network. The compromise may be maintained for years, growing in scale and complexity over time.'[39]

6.51. The TSRs seek to segregate critical management functionality from networks with direct access to the internet and ensure that management is performed securely.

6.52. In particular, NCSC note that this would include a Privileged Access Workstation (PAW) model where a set of workstations are used to manage specific equipment and administrative staff gain access in a safe way.

6.53. This is likely to result in both equipment costs and increased staff costs for operators as new workstations are required and staff are required to follow new processes to access them. Input from operators indicates that this will be one of the most significant cost impacts.

The signalling plane

6.54. Signalling networks connect public telecoms networks. They allow operator networks to connect to each other, reach each other's services and ultimately allow users to communicate with each other.

[38] ibid

[39] ibid, section 5.2.

6.55. NCSC found that ‘traditionally, and to a degree currently, telecoms standards have been built on an assumption that all signalling from other telecoms networks can be trusted. However, that assumption is no longer valid as these international networks can be exploited by attackers to conduct attacks.’[40]

6.56. The TSR seeks to ensure that operators consider that any inbound signalling may be malicious and treat it appropriately. The intent is to increase the network’s resilience to disruptive attacks from external signalling networks, and to inhibit the leaking of subscriber or network data over external signalling networks.

6.57. The costs of these requirements will depend on an operator's existing processes but will likely include process redesign and implementation costs, ongoing costs of supporting and monitoring new processes including any associated equipment costs.

The virtualisation plane

6.58. Virtualisation refers to the creation of a virtual resource such as a server, desktop, operating system, file, storage or network.[41] It is a widely used technique in the telecoms industry.

6.59. The NCSC found that in telecoms networks, ‘compromise of the virtualisation fabric could result in an impact to the network availability, or full compromise of the operator’s core and all workloads running within it. A successful ‘virtual function to physical host’ attack could enable an attacker to bypass the hypervisor’s enforced separation, allowing the attacker to influence and control any workloads running on the impacted host.’[42]

6.60. The TSR contains requirements for the virtualisation plane that cover three areas:

- Hardware mitigations which apply to CPU[43] manufacturers
- Software mitigations relating to the hypervisor operating system
- Architectural mitigations to securely architect the virtualised infrastructure.

6.61. The costs of these requirements will depend on an operator's existing processes but could include process redesign and implementation costs, ongoing costs of supporting new processes including any associated equipment costs.

The supply chain

6.62. The NCSCs TSR included a number of requirements relating to the supply chain. These requirements seek to mitigate the following supply chain risks:

- equipment quality and security issues;
- supplier network access and support; and
- operator data, including SIM supply.

6.63. To mitigate these risks the TSR address a number of areas[44]:

[40] ibid, section 5.3.

[41] Techopedia, https://www.techopedia.com/definition/719/virtualization.

[42] Summary of the NCSC’s security analysis for the UK telecoms sector, 2020, Section 5.4.

[43] Central Processing Unit.

[44]Summary of the NCSC’s security analysis for the UK telecoms sector, 2020, Section 7.5.

- Supply chain governance: These requirements seek to ensure that operators impose obligations onto their supply chain to enhance security. As a first step operators are expected to understand their supply chain risks and then to manage those risks by placing security requirements onto suppliers and ensuring that suppliers place requirements on their supply chain in turn.
- Administration and management of Third Party Administrators (3PAs): The TSRs require that, where a third party is providing administrative functions, they should be subject to the same security controls as those in operation at an operator itself (as described in 'The management plane' above). This means that managed service providers (MSPs) should appropriately segregate the systems used to access operator networks, ensuring that compromise of the MSP does not compromise multiple operators. It also means that operators would be required to limit access into their network, both in terms of scope and time for MSPs.
- Equipment quality and security: The TSRs expect operators to require vendors to publish detailed security white papers and the NCSC has provided detailed guidance on the information that operators should request from vendors to allow security assessments to be conducted, and the tests that can be performed to verify these assessments. Operators would also be required to cost-in security risk into their procurement activities.
- Protection and sharing of data: The TSR set requirements relating to data ownership, transfer and data access. For example, when technically possible, data accessed by a third party is required to be anonymised and obfuscated.[45]
- Protection of User Access Credential data: User access credentials, such as SIMs, should be protected and this information only held within the operator.

6.64. These requirements could generate a range of costs:

- Supply chain governance could result in additional procurement costs both procedural and in terms of cost of supply.
- Administration requirements could require real-time oversight of the 3PA's network access as well as time spent on security investigations and preemptive oversight of appropriate logs and audit data.
- Requirements on vendor security could also generate procurement and oversight costs.
- Data requirements could generate process design and ongoing data handling costs.

6.65. Input from operators has indicated that the breadth of supply chains means that the costs of administering these requirements could be significant.

[45] Protection of data under the TSR is not limited to personal data/sensitive personal data as covered by data protection legislation (e.g. the Data Protection Act 2018) but also includes systems data and corporate data.This data - which is critical to the running of telecoms companies and the functioning of the network - is not necessarily covered by that existing legislation.

Retaining national resilience and capability

6.66. The NCSC set out the intent of the TSR in this area as ‘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 TSR aims 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, from damaging UK networks.’[46]

6.67. This is an area where operators have highlighted potential costs including costs relating to designing and putting in place the relevant oversight processes. These could include:

- assessing UK-based capabilities to ensure network resilience and the ability to continue to operate a network in response to a prolonged interruption to international connectivity or loss of offshore technical/operational support;
- reconfiguring internal processes to ensure security investigations can be carried out from within the UK; and
- onshoring management hardware to the UK.

Assurance costs

6.68. Sections 105A-D (security of public electronic communications networks and services) Communications Act 2003 provides the current legislative framework for telecoms security, overseen by Ofcom. It provides that all telecoms operators must take technical and organisational measures to appropriately manage security risks. New legislation will look to enhance this framework, to level up security across the industry.

6.69. Ofcom has published guidance to assist telecoms operators (ie PECN and PECS) in complying with their current obligations under the Communications Act. In issuing this guidance Ofcom is “encouraging compliance by explaining the security and resilience (statutory) obligations imposed on relevant communications providers, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns.”

6.70. Ofcom’s approach to overseeing compliance with the current legislative framework for telecoms security set out in the Communications Act 2003 is to monitor ex post through reports of breaches and auditing a network or service providers security measures where necessary.

6.71. The Security Framework will be regulated using a self reporting model. Companies will be required to provide Ofcom with information that sets out how they comply with their overarching security duty set out in primary legislation, having reference to any Code of Practice issued by the Secretary of State.

6.72. In addition to self reporting Operators would be required to submit to spot checks, that could include attending their physical premises, to confirm the veracity of their

[46] ibid, Section 7.6.

compliance reporting. These checks would not be full audits of compliance but related to parts of the reporting.

6.73. The costs of this assurance framework will depend on the frequency of compliance reporting, and the style of this compliance reporting which would be set out by Ofcom. We have not estimated these costs for the purpose of this Impact Assessment.

6.74. In order to understand costs to industry we consider it would be necessary to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

Costs incurred by other operators

6.75. Under the proposed Telecoms Security legislation communications providers must demonstrate to Ofcom how they comply with the security duties and sub duties set out.

6.76. We are proposing a tiered approach to the Codes of Practice, where larger operators were expected to take a greater level of measures (which will largely mirror those set out in the current NCSC Draft TSR) smaller operators will have to follow a subset of these measures. This detail would be set out in the Codes of Practice.

6.77. Whilst non Tier 1 operators are not expected to implement the full Code of Practice in the same way as Tier 1 operators, we expect that the subset of measures that will apply to smaller operators will have an impact on these operators and the costs that they incur.

6.78. The NCSC TSR - as described above - is more prescriptive than the existing Ofcom guidance insofar as it includes specific principles, requirements and tests which are not included in the existing guidance.

6.79. Therefore, in addition to familiarisation costs, we expect that non Tier 1 operators will incur costs in complying with the new security duties. We expect that the type of costs incurred will be similar to those incurred by Tier 1 operators which are set out above but that depending on the scope of the Code of Practice for these operators the scale of costs could be lower.

Monitoring costs

6.80. Ofcom already has responsibility for oversight of provisions of the CA which require network operators 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.[47]

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

6.82. Ofcom will incur some costs under the 'do nothing' scenario where TSRs published by NCSC as guidance are in place. These include:

- updating existing s105A-D guidance to reflect NCSC's TSR as best practice guidance;

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

- working with providers to undertake an analysis of the gap between their current security arrangements and those set out in the NCSC's TSR.

6.83. As a result of the Telecoms Security Bill Ofcom will be given an expanded security duty to regulate this system, taking regard of the Code of Practice in their regulatory work.

6.84. The Department for Digital, Creative Media & Sport (DCMS) will also incur additional costs as a result of this legislation. DCMS is considering creating a new 'oversight and enforcement' team which would provide administrative support for the SoS under the new security regime.

6.85. It is expected that both Ofcom and DCMS will incur costs in carrying out these functions. We estimate these costs in Table 2 below based on information provided by both Ofcom and DCMS in May 2020. These 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, using a 25% discount on the base estimates to find the low estimate and a 25% load to find the high estimate. The final cost will depend on the detail of implementation and is subject to continuing discussions with HM Treasury as Ofcom work towards approval of final required spend.

6.86. These costs relate to the costs of regulation of the TSR; other costs will be incurred with respect to the national security powers in relation to high risk vendors:

Table 2 - Costs of monitoring compliance with National Security legislation

	Costs of monitoring compliance with the telecoms security requirements	
	Total costs in net present value terms over the period 2020 - 2029 (3.5% discount rate), £m	
	Low estimate	High estimate
Ofcom costs	29.6	49.4
DCMS costs	0.8	1.4
Total	30.5	50.8

Impact on justice system

6.87. Ofcom will be given an expanded security duty to regulate this system, taking regard of the Code of Practice in their regulatory work.

6.88. This will broadly be using a self-reporting mechanism - operators 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 operators is accurate.

6.89. 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 will be set out in the Justice Impact Assessment. The current appeals system will be utilised.

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

Economic Impact - benefits

6.91. This section details the potential economic benefits of improving the security and resilience of 5G and full fibre networks in the UK through the Telecoms Security Bill.

6.92. The Telecoms Security Bill seeks to address the security concerns set out in the Review through two sets of measures: the Telecoms Security legislation which is the subject of this Impact Assessment and the national security powers in relation to high risk vendors. The objectives of these measures is set out above in the section The Telecoms Supply Chain Review. As both of these measures set out to address the same underlying concern it is not surprising that the benefits of these measures are similar and the benefits that we set out in this section should be considered across both measures.

6.93. A 2018 Ericsson report[48] found that the two main barriers to 5G adoption are concerns around data security and privacy and lack of standards. This is backed up by a 2016 survey by Qualcomm of telecoms experts, in which 58% of respondents said ‘The widespread adoption of 5G over the next decade is not possible without strong security and enhanced protections for sensitive data’[49].

6.94. We consider that the economic benefit arising from 5G use cases, where network security and resilience are considered a prerequisite to their adoption, likely to be the key economic 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 Telecoms Security legislation - we do not have any information on which to base such an assumption.

6.95. In addition we also 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.

Evidence of current vulnerabilities in the network

6.96. As set out 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

[48] Ericsson report - Industry Impact of 5G 2018.pdf
[49] 5G Economy Global Public Survey Report Commissioned by Qualcomm

the enabling infrastructure that drives future economic growth. The next few years will see increased investment in these networks, with the first 5G consumer services launched in May 2019 and over half the country expected to get full fibre connections by 2025. The security of these networks is in the UK's economic interest'.[50]

6.97. The NCSC has been at the forefront of protecting the UK from online threats, handling well over six hundred incidents in 2019 alone.[51]

6.98. 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 most recent Cyber Security Breaches Survey, undertaken by Ipsos Mori and published by DCMS in March 2020[52]. 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.

6.99. Certain types of cyber attacks seem to be particularly aimed at telecommunications companies. 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[53].

6.100. EfficientIP's 2017 Global DNS Threat Survey Report, which surveyed 1,000 global telecoms operators and vendors, states that 25% admitted they have lost sensitive customer information as a result of a DNS attack[54]. This is higher than any other sector surveyed.

6.101. For 42% of telecoms companies surveyed, attacks resulted in in-house application downtime, which caused poor customer experience online.

6.102. In January 2020, the NCSC published a report detailing the findings from their extensive analysis of the security of the telecommunications sector[55]. 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 operators' management plane
- Exploitation via the international signalling plane
- Exploitation of virtualised networks
- Exploitation via the supply chain
- Loss of the national capability to operate and secure our networks (dependency)

6.103. In the same report the NCSC 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

[50] UK Telecoms Supply Chain Review Report
[51] The NCSC Annual Review 2019
[52] Cyber Security Breaches Survey 2020: Statistical Release, 2020
[53] https://www.nexusguard.com/threat-report-q3-2018, 2018
[54] https://www.efficientip.com/dns-security-telecom-sector/, 2017
[55] Summary of the NCSC's security analysis for the UK telecoms sector, 2020

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. Using an MSP in this way, as a platform to attack multiple further targets, demonstrates why this risk is of concern.

6.104. 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 (2G, 3G and 4G). The failure affected all of O2's MVNOs such as Tesco, Sky, giffgaff and Lycamobile. Voice and SMS services were impacted too. 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.[56]
- 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.[57]
- 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. The incident occured over 5 days, with no known cause or outcome.[58]

Costs of security incidents

6.105. In terms of costs, there is a significant range across the literature and case studies. 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.

6.106. Efficient IP's survey, which only looks at the telecoms sector, states that each attack on a network costs an average of £460,000 to remediate, with an average of 3 employees spending over 17 hours per attack. Furthermore, 5% of telecoms organizations surveyed stated an attack cost them more than £3.75 million.

6.107. Of the case studies discussed above, only the TalkTalk case study set out above has an associated cost attached to it. The total cost to TalkTalk was £60m,

[56] https://www.theregister.co.uk/2018/12/06/ericsson_o2_telefonica_uk_outage/

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

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

including a fine of £320,000 to the ICO, consumer compensation and costs associated with reputational damage.

6.108. 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 £60m. Therefore the benefit of this legislation preventing one security incident could lie within the same range. Unfortunately, the case studies and data that are available on the cost of telecoms security incidents is not substantial enough to reduce that range. Very few costs have been monetised for security incidents in the telecoms sectors and of those that have, the figures are not sufficiently comparable.

6.109. Since we are not able to use the data available to estimate the cost of a cyber incident in the telecoms sector, the benefit of reduced cyber incidents has not been included in the monetised benefits of this impact assessment. However, it is clearly an important benefit of the TSR legislation and reducing the number and impact of cyber incidents would benefit both operators and consumers of telecoms services.

Telecoms Security legislation will improve operator security levels

6.110. In their security analysis for the UK telecoms sector, the NCSC state how they expect the Telecoms Security Requirements to improve the security of the sector. This extract is shown in Box 5.

Box 5 - NCSC Background on Telecoms Security Requirements[59]

No system can be 100% secure or available. The intent of the TSRs is to set realistic standards for the protection of our national telecoms networks and to clarify the security offer from operators to their stakeholders, whether they be users, government, the regulator or other operators. Through practical controls, we want to make it hard for an attacker to compromise a UK network, make it likely that any such compromise will be noticed quickly and the harm and impact limited, and make remediation as simple as possible. These are commercial networks, and security of those networks has to be judged in the context of commercial realities. This is all independent of any given threat actor; our aim is to protect equally from them all.

Consequently, the TSRs define an achievable baseline of security controls to protect operator networks from realistic and nationally significant cyber attacks.
The TSRs are presented within a broader framework that describes the risk that motivates the requirement, and guidance on the implementation and testing of the requirement. The TSRs have been built around mitigating the five main areas of significant risk:

- management plane
- signalling plane
- virtualisation plane
- supply chain
- loss of national capability to operate UK networks

The requirements aim to provide a consistent, measurable, and achievable list of security controls and procedures that will help improve the security of all UK telecoms networks when applied together.

The TSRs set out all recommended security controls, even the most basic. Security controls are not consistent across the industry and including even the most basic controls in the TSRs ensures an essential control is not missed. Adopting the TSRs will improve the security of the UK's national telecommunication sector, building confidence in the security and resilience of our telecoms services.

6.111. The Telecoms Security legislation will help harden the network against attack, reduce security risks by reducing the impact of a cyber attack or network outage. This could mean a reduction in the number of successful attacks and/or a fall in

[59] Summary of the NCSC's security analysis for the UK telecoms sector, 2020, Paragraph 7.1.

the cost of an attack as attacks are noticed more quickly and remediation is simpler.

Economic benefits of 5G and Full Fibre

6.112. 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.' [60]

6.113. We have estimated the economic benefits of 5G and full fibre-to-the-premises broadband (FTTP) networks over the next 8 years based on five industry reports which estimate the economic benefits produced.[61,62] The key results are detailed below[63].

Table 3: Estimated economic benefits of 5G and full fibre broadband, discounted over 8 years at a 3.5% discount rate

	Economic benefits through to 2025	**Economic benefits through to 2028**
5G	c.£78bn	c.£137bn
Full Fibre	c.£184bn	c.£324bn
Combined	c.£262bn	c.£461bn

6.114. The modelling shows a combined benefit of £461bn to the UK over the next 8 years. This is the total economic benefit generated by 5G and full fibre. 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 TSR legislation, the full extent of these benefits will not be realised.

[60] UK Telecoms Supply Chain Review Report, 2019

[61] The analysis has not been updated to take into account the potential impact of the Covid-19 pandemic, and does not include the potential impact of the Telecommunications Security Bill.

[62] The benefits arise from a number of factors - the returns and multiplier effects from 5G and Full Fibre investments including employment, and the wider benefits from the utilisation of 5G and Full Fibre services including productivity gains to producers (eg Automotive, Healthcare, Utilities, Transport, etc) and to consumers and workers.

[63] We have estimated the benefits to the UK economy from 5G and FTTP rollout based on available literature. Estimates of the economic benefits of 5G are uncertain at this stage. Our analysis of different sources suggests that potential benefits of 5G in 2025 could be around c.£25bn (with a range from c.£13bn to over £40bn), and c.£59bn for FTTP. We have assumed a linear increase in annual benefits over the period 2019-2025 (with no benefit in 2019), and we have assumed that benefits are flat after 2025 (when commercial rollout is expected to be completed).

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

6.115. From our literature review of twelve reports published over the last 4 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.

6.116. 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 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.’[64]

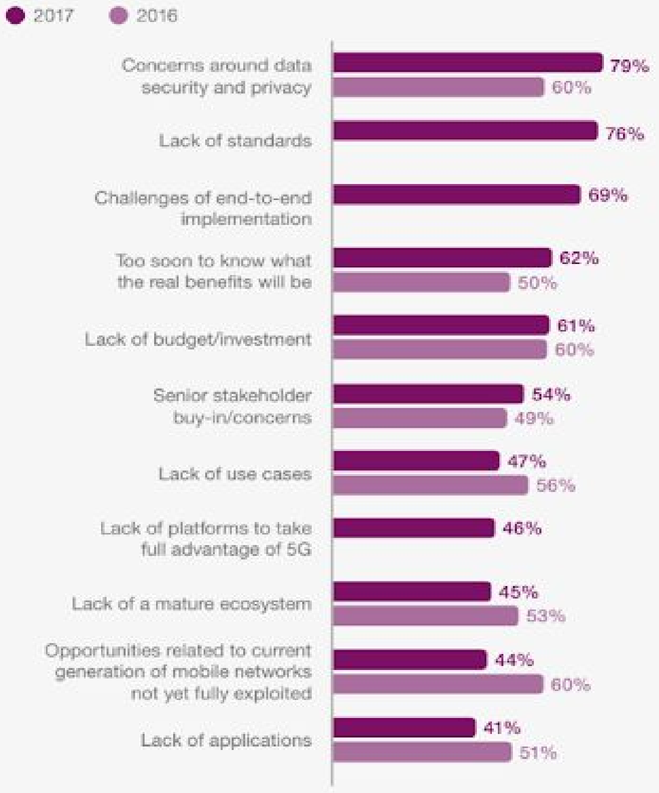
6.117. The literature shows that some of the use cases rely heavily on networks that are highly secure and reliable. This is backed up by the finding in a 2018 Ericsson report[65] that the two main barriers to 5G adoption are concerns around data security and privacy and lack of standards. This is demonstrated in Figure 1.

Figure 1: Key barriers to adoption of 5G

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

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

Figure 8: Key barriers to adoption of 5G



Source: Ericsson

6.118. Telecoms Security legislation 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 Telecoms Security legislation 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.

6.119. Therefore the quantifiable benefits of the Telecoms Security legislation 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 4 use cases. We have estimated the economic value of these cases.

6.120. The Ericsson report highlighted the 4 use cases with a particular reliance on secure and reliable 5G networks:

1. Remote health examination and monitoring
2. Remote robotic surgery
3. Autonomous cars
4. Automated threat detection

6.121. This is backed up by a 2016 survey by Qualcomm which conducted 3,500 interviews across industry players, academics and experts from telecoms and the relevant vertical sectors[66]. 58% of respondents said ‘The widespread adoption of 5G over the next decade is not possible without strong security and enhanced

[66] 5G Economy Global Public Survey Report Commissioned by Qualcomm

protections for sensitive data'. The three use cases where cyber security was identified as most important were:

1. Safer autonomous vehicles
2. Improved emergency response
3. Increased access to virtual medical care

6.122. In order to monetise these benefits, we have set out the three use cases for which we were able to find robust estimates of future economic benefit in the table below.

Table 4: Monetisable benefits of each 5G use case, discounted at 3.5% over 10 years

Use case	Economic benefit (£bn)
Remote medical examination	8.5
Remote health monitoring	8.9
Autonomous cars	3.8
Total (2020-29)	21.1

6.123. The total monetisable benefits of the three identified use cases between 2020 and 2029 is estimated to be £21.1bn, in present value terms.

6.124. These values are based on estimated economic benefits and deployment timelines for each use case. We set out these estimates below: as found in the literature.

Remote medical examination (Economic Benefit: £8.5bn)

6.125. 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'[67]

6.126. A 2019 report from Cambridge Wireless states that 'the ability to maintain uninterrupted communication will be invaluable for many telemedicine applications'. Specifically for medical examination, '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.'[68]

6.127. 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

[67] Ericsson's 5G Business Potential report

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

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.[69]. 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.'[70]

6.128. Analysts at Global Market Insights predict the use of telehealth will triple by 2025, fuelled largely by 5G[71]. The same report states that the 'Teleconsultation service market is expected to grow at 18.9% CAGR across the forecast timeframe.'[72].

6.129. Our analysis of the economic benefits of remote medical examination starts with the £1.3bn benefit expected in 2025, based on the assumption that that 5G penetration will be close to 100% in UK cities from the O2 report. Taking this with the Global Market Insight finding that the market will triple by 2025, and the requirement for operators to comply with the legislation by 2023, we have assumed that the benefit will increase linearly from £0 in 2023 to £1.3bn in 2025. Beyond 2025, we have assumed the 18.9% CAGR growth rate reported above.

Remote health monitoring (Economic Benefit: £8.9bn)

6.130. When we refer to remote health monitoring devices, we are talking about devices that are connected to the internet, also known as 'Internet of Things' devices. Traditionally non-internable physical devices are beginning to be embedded with technology that allows these devices to communicate and interact over the internet. 5G greatly improves what businesses can do with IoT devices, as summarised in a 2019 GSMA report:

> 'Although 4G will continue to be used for many consumer and enterprise IoT use cases, 5G provides a range of benefits to the IoT which are not available with 4G or other technologies. These include 5G's ability to support a massive number of static and mobile IoT devices, which have a diverse range of speed, bandwidth and quality of service requirements.'[73]

6.131. A 2010 report from the University of Agder in Norway summarised how 5G can improve and enable remote patient monitoring:

> 'Within a future 5G infrastructure, new possibilities will be available due to improved addressing solutions and extended security services in addition to higher bandwidth in the wireless communication link. Thus 5G solutions can represent a paradigm shift regarding remote patient's monitoring and tracking possibilities, with enhancement in transmitting information between patients and health care services'.'[74]

The O2's 2018 report estimates that health monitoring devices will reduce

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

[70] NHS Long Term Plan v1.2 August 2019

[71] Global Telemedicine Market size to exceed $130.5 Bn by 2025

[72] Telemedicine Market By Service Type, Component and Deployment | Forecast 2023

[73] Internet of Things in the 5G Era, GSMA

[74] Remote Patient Monitoring Within a Future 5G Infrastructure, Oleshchuk and Fensli, 2010

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[75]. We have assumed that both use cases require secure and reliable networks, with a potential annual benefit of £1,353 million by 2025[76]. This is a lower estimate than the one produced 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.[77]

6.132. 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[78].

6.133. Our analysis of the economic benefits of remote medical monitoring starts with the £1.3bn benefit expected in 2025, based on the O2 report. 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).

Autonomous cars (Economic Benefit: £3.8bn):

6.134. TechRadar summarises why 5G is requirement when it comes to autonomous cars in a June 2019 article:

> ‘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.’[79]

6.135. A 2015 KPMG report on connected and autonomous vehicles estimates the overall economic and social benefit of such vehicles could be in the region of £51 billion per year by 2030[80]. If we make a (conservative) assumption that 10% of the estimated benefits from CAV development comes from autonomous vehicles, we come to a benefit of £5.1bn per year by 2030.

6.136. The literature is varied in its estimates of when CAVs will begin to hit the market. The Department for Transport announced in February 2019 that a process was being developed to support advanced trials of automated vehicles. The announcement from DfT stated that this ‘demonstrates that the government is on track to meet its commitment to have fully self-driving vehicles on UK roads by 2021’[81]. However, Emerj, an AI research and advisory company, forecasts a different outcome.

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

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

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

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

[79] 10 things 5G can do that 4G can’t

[80] Connected and Autonomous Vehicles – The UK Economic Opportunity

[81] Government moves forward on advanced trials for self-driving vehicles

6.137. In a March 2020 report, they concluded that 'although in 2016 many industry leaders expected autonomous vehicles to be commonplace on highways in the early 2020s, this doesn't seem likely… Now that the conversation around AI in the enterprise is more informed, executives are walking back their initial statements because they understand how difficult machine learning projects are in general, let alone those for self-driving cars.'[82]

6.138. Another government publication, Road Traffic Forecasts 2018[83], forecasted the years that different levels of connected and autonomous vehicles enter the market between the late 2020s and late 2040s.

6.139. Given the above, it is reasonable to assume that autonomous vehicles will not be available in the market until late 2020s, so benefits will likely not start to accrue before this. Therefore we have assumed that the market will experience linear growth between 2028 and 2030, reaching an annual benefit of £5.1bn in 2030.

Sensitivity analysis and benefits illustration

6.140. We have conducted some sensitivity analysis on these total benefits to illustrate the impact of varying our assumptions. We have modelled a scenario where the deployment of these use cases are delayed by two years. In this case, the total monetisable benefit, discounted at 3.5% over the next 10 years, falls to £9.4bn. 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.

6.141. Furthermore, not all of these benefits can be attributed to the Telecoms Security Legislation. 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 (for reasons listed previously).

Direct costs and benefits to business calculations

6.142. Familiarisation costs and costs of regulation are quantified above. However, these costs are likely to be a relatively small proportion of total costs and we note that further work is required to understand familiarisation costs.

6.143. Whilst we have not been able to carry out a structured assessment of costs to operators, feedback from bilateral discussions with Tier 1 operators have indicated that the costs of implementing the NCSC TSR would be significant. The scale of these costs is likely to differ by size of operator and could be of the scale of over £10 million in one off costs and the same magnitude of ongoing costs (over the

[82] The Self-Driving Car Timeline – Predictions from the Top 11 Global Automakers

[83] Road Traffic Forecasts 2018

impact assessment period) for an approximately median sized operator. These indicate potentially significant costs. However, we note that there is a large degree of uncertainty on the level of potential costs - which reflects the uncertainty over the final scope of the NCSC's draft TSR and the changes that operators will need to make as a result of this legislation.

6.144. In addition there is also uncertainty about:

- the implementation timetable for the Code of Practice and Telecoms Security legislation more broadly; and
- the contents of the Code of Practice itself.

6.145. As a result, and due to the reasons set out in section Rationale and evidence to justify the level of analysis used in the IA (proportionality approach) we have not indicated an estimate of total costs in our impact assessment. In order to understand total costs we consider it would be necessary to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures.

6.146. On the other hand there are significant benefits of the TSRs and these benefits are far reaching across the telecommunications sector. We have focused on two types of benefits where we are able to estimate the economic impact best. These are the benefits of:

- Unlocking 5G use cases
- Reducing security risks

6.147. Of these benefits the most significant - in absolute terms - is unlocking 5G use cases. We have found that for three use cases where cyber security was identified as important (safer autonomous vehicles, improved emergency response and increased access to virtual medical care), there are monetisable benefits of £21.1bn between 2020 and 2030, as a net present value.

6.148. Not all of these benefits can be attributed to the TSR legislation. 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 capital are also required.

6.149. The analysis of 5G use cases is focused on a small number of use cases. But there are also wider benefits associated with the rollout of full fibre and 5G networks - we estimate a combined benefit of £461bn to the UK over the next 8 years in Table 3 above. These wider benefits of the rollout of these networks may include additional use cases for which security is important which would indicate a set of much larger potential benefits. As such our analysis - with respect to the benefits of 5G use cases - should be considered an illustration of some of the benefits that we can monetise.

6.150. Whilst we have monetised potential benefits from unlocking 5G use cases - and the wider benefits of 5G and full fibre networks. 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 Telecoms Security legislation - we do not have any information on which to base such an assumption.

6.151. As an illustration we have modelled three possible scenarios for the proportion of the benefits of the 5G use cases that we identified that could be attributed to the Telecoms Security legislation. These scenarios are illustrative as we do not have any information that would enable us to estimate this proportion. Table 5 shows that if we can attribute 5% of the benefits of the 5G use cases we identified, in section TSRs will unlock 5G use cases above, to the Telecoms Security legislation we could identify benefits of over £1bn. As we have not been able to estimate the costs of implementing the Telecoms Security legislation we cannot say whether benefits of this scale would be commensurate with the costs of implementing the framework. However, it does indicate that we would only need a very low proportion of the benefits of 5G to be attributable to improved security for the benefits to be considerable.

6.152. We will expand on this analysis as we develop our cost estimates, and conduct 'breakeven' analysis to say what proportion of the benefits of 5G would need to be attributable to improved security for those benefits to equate to the costs of the policy.

Table 5: Illustrative proportion of total 5G use case benefits realised due to the Telecoms Security Legislation

% of total benefits realised	**1%**	**5%**	**10%**
PV of benefit (£bn) (best estimate for total benefits)	0.2	1.1	2.1

6.153. We have outlined some of the monetisable benefits of improving security in the UK telecommunications above. However, this analysis is unlikely to be able to capture all of the wider security benefits of these measures.

6.154. The NCSC's threat analysis has highlighted that our telecoms sector is potentially vulnerable to a range of cyber risks and that this analysis was backed up by evidence generated from security testing of telecoms networks and by security incidents.

6.155. We cannot know what will happen if this legislation is not taken forward, apart from the economic activity that we believe is facilitated by this legislation, the legislation is also intended to reduce our vulnerability to cyber risks. The potential costs of an attack are broad - and there may be an unprecedented incident the costs of which we cannot seek to measure at this time. However, the TalkTalk cyber hack, costing £60m in total, can serve an illustrative example of the potential cost of one cyber incident in the telecoms sector. The Telecoms Security legislation will help harden the network against such an attack, reduce security risks by reducing the impact of a cyber attack or network outage; this should be considered as an unquantified benefit in addition to the economic benefits outlined.

7. Impact on small and micro businesses

Into what sector and/or subsector the affected businesses fall

7.1. In the UK communications providers are regulated, primarily, by the Communications Act 2003. Communications providers are companies who carry content services either over their own network (a Public Electronic Communications Network or PECN) or using another Communications Providers network (a Public Electronic Communications Service or PECS).

7.2. Examples of Communications Providers include[84]:

- Fixed-line owners and operators (such as British Telecommunications (BT) and Virgin Media).
- Mobile network operators (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 operators (such as Virgin Mobile) who do not own their own network but use networks belonging to MNOs.
- 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; cable (Virgin Media); or satellite (Sky).
- VoIP (voice over internet protocol) operators (such as Skype).
- Satellite network providers (such as Sky).
- Broadcast network providers (such as Arqiva).

Number of businesses in scope of the regulation

7.3. PECN and PECS are not required to hold a licence to operate because they are Generally Authorised to operate if they comply with a set of General Conditions which are drawn up and are enforced by Ofcom under the Communications Act. For this reason Ofcom does not hold a list of all companies that fall within the PECN and PECS categories.

7.4. Ofcom does hold some information on the number of PECN and PECS where they:

- Have applied for Code powers which enable providers of telecommunication services, subject to necessary planning requirements, to construct infrastructure on public land (streets), to take rights over private

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

land, either with the agreement of the landowner or by applying to the County Court[85]

- Have paid administrative fees to Ofcom because they have relevant turnover (turnover made from carrying on any Relevant Activity[86] after the deduction of sales rebates, value added tax and other taxes directly related to turnover) over £5m.

7.5. As of 3rd March 2020, 176 companies were listed on Ofcom's website as having applied for Code powers with Ofcom. In 2019/2020 119 companies were listed as having paid administrative fees to Ofcom. This gives an estimate of the number of PECS and PECN of at least 176, with a number of those being small and medium sized businesses based on relevant turnover.[87]

7.6. However, there may be more PECN and PECS who are covered by Ofcom's General Authorisation regime but not included in these lists. These are most likely to be small and micro businesses as they would need to have a relevant turnover of under £5m.

7.7. ONS data on number of businesses by turnover indicates that there are a large number of of small and micro businesses in the Telecommunications sector[88]. Table 6 below sets out the number of businesses providing telecommunications services by turnover band[89]. These businesses are likely to include, but not be limited to, PECN and PECS. This indicates that there could be a sizable long tail of small and micro businesses that are Generally Authorised to operate under the Communications Act 2003.

Table 6 - All VAT and/or PAYE based enterprises within the UK, under the Telecoms SIC code, by employment size bands

Industry	Micro (up to £2m)	Small (£2-5m)	Small (£5-10m)	Medium (£10-50m)	Large (£50m+)
61100 : Wired telecommunications activities	1,615	55	20	15	5
61200 : Wireless telecommunications activities	1,415	50	30	25	10
61300 : Satellite	125	10	10	5	5

[85] As of 3rd March 2020, **176** companies were listed on Ofcom's website as having applied for Code powers with Ofcom. Full list can be found here.

[86] Relevant activities: 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.

[87] Relevant turnover may not include some business activities so a PECN/PECS with Code powers that does not pay administrative fees could have a total turnover over £5m.

[88] Telecommunications: This division includes the activities of providing telecommunications and related service activities, that is transmitting voice, data, text, sound and video. The transmission facilities that carry out these activities may be based on a single technology or a combination of technologies. The common feature of the activities classified in this division is the transmission of content, without being involved in its creation. The breakdown in this division is based on the type of infrastructure operated.

[89] Turnover provided to the ONS for the majority of traders is based on VAT returns for a 12-month period. The figures represent total UK turnover, including exempt and zero-rated supplies.

telecommunications activities					
61900 : Other telecommunications activities	4,420	265	120	145	70

Source: ONS Inter-Departmental Business Register (IDBR)

Do the impacts fall disproportionately on small and micro businesses?

7.8. The RPC guidance on small and micro business assessments sets out the economic intuition behind the assessment as:

"The economic intuition behind SMBs being disproportionately affected by regulation is that some costs resulting from complying with regulation are fixed, i.e. they do not depend on the output of the business. Since larger businesses operate on a greater scale, such fixed costs are likely to be a smaller proportion of their overall costs."[90]

7.9. High fixed costs are particularly prevalent where regulations may require a fixed number of hours for operators to familiarise themselves with a set of rules or establish new business processes.

7.10. We know that there are likely to be significant familiarisation costs associated with the TSR and that these are a fixed cost which will create a disproportionate impact on small and micro businesses.

7.11. We also know that familiarisation costs are likely to be a small proportion of total costs. DCMS has been present during engagement between NCSC and operators on the TSR and through this participation has understood that some elements of the TSR could create significant costs for industry but that this may vary between operators whose networks have different characteristics.

7.12. At this stage we have limited information on the direct costs to business of the TSR. We expect that other costs would include:

- Process design costs
- Equipment costs
- Procurement and supplier management costs
- Assurance costs

7.13. As discussed in section Rationale and evidence to justify the level of analysis used in the IA (proportionality approach) above. DCMS intends to engage extensively with industry and wider stakeholders in advance of laying secondary legislation including further work to understand the costs to business that will result from these measures. We also propose that we will consult with industry in the policy development process for the final Code of Practice.

7.14. This approach will also allow us to consult widely giving all PECN and PECS the opportunity to input information.

7.15. It is useful to note that the seven largest operators hold 88% of the total fixed telecoms market in the UK. In the mobile network, this is even more pronounced, with just four network operators making up circa. 85% of the mobile network. The market share of each of these operators are shown in tables 7 and 8.

[90] Small and Micro Business Assessments: guidance for departments, with case history examples

Table 7: Mobile network market shares by subscribers at 31 December 2017

Operator	Market share
BT / EE	28%
O2	26%
Vodafone	21%
Three	12%
Tesco Mobile	6%
Virgin Mobile	4%
TalkTalk	1%
iD Mobile	1%
Sky	1%
Others	<1%

Source: Statista[91]

Table 8: Fixed network market shares by broadband subscribers at 2018

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

Source: Statista[92]

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

Could SMBs be exempted while achieving the policy objectives?

7.17. We do not consider an exemption would be appropriate. Customers of telecoms operators 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.

7.18. Existing security duty on PECN and PECS (s105A requirement to protect security of networks and services) to ensure they have 'appropriate measures' in place to manage security applies universally, including to small and micro PECN and PECS. These obligations are derived from the European Union's common regulatory framework for electronic communications networks and services (the Framework).

[91] UK: Mobile network market share 2018

[92] • UK telecoms operators: broadband subscribers share 2018

7.19. To assist PECNs and PECSs Ofcom already published guidance which is based on the requirements of the Communications Act. In issuing this guidance Ofcom is "encouraging compliance by explaining the security and resilience (statutory) obligations imposed on relevant Communications Providers, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns."[93]

7.20. The Act contains duties under three headings:

- Protecting security
- Breach notification
- Auditing and enforcement

7.21. Under these headings Ofcom set out guidance on how PECNs and PECSs are expected to comply with their obligations. In the guidance Ofcom notes that "the measures it would be appropriate for a large Communications Provider to take to protect security may be different to those appropriate for a smaller company. It is for Communications Providers in the first instance to assess for themselves (taking this guidance into account) the measures which are appropriate in their own particular cases.'[94]

7.22. This illustrates that the current arrangements recognise the need for a proportionate approach depending on the size of the company.

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

7.23. We consider a mitigation would be appropriate. Whilst we're seeking to strengthen the overall arrangements, we're retaining that recognition of proportionality depending on the size of the company that is currently in place.

7.24. We will seek to apply a tiered approach to mitigation in which one Code of Practice will apply to larger operators. Proportionality will be ensured in the mitigation model through having only applying subsequent, less detailed Codes or high level duties for smaller companies.

7.25. The approach to determining which operators are in scope of the full Code of practice will be subject to public consultation.

.

[93] Paragraph 1.5.

[94] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003 2017 Version, paragraph 1.10.

8. Competition impacts

8.1. In line with the competition impact assessment guidelines we have considered whether the Telecoms Security Legislation is likely to have an impact on competition by considering the following questions:

- 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

8.2. We consider these questions in turn first noting the market structure of the downstream UK telecommunications market.

Downstream UK telecommunications market

8.3. In the UK mobile sector there are four mobile network operators ("MNOs")—Vodafone, EE, O2 and Three, as well as numerous MVNOs (mobile virtual network operators). 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 providers network.

8.4. 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.

8.5. 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

8.6. The legislation will raise the height of the security bar and require telecoms operators, overseen by Ofcom and Government, to design and manage their networks to meet the new duties. The Code of Practice will provide clarity to industry on what is expected in terms of network security.

8.7. It is not expected that this legislation would affect the number of these networks because; the operators required to implement the full Code of Practice are large organisations who already have significant security and resilience functions and have the capacity to implement the TSR; and the NCSC has consulted these operators on it's TSRs - on which the Code will be based - in draft version to ensure that they can be implemented by operators.

8.8. With respect to non-Tier 1 operators given the high level nature of the duty (and reduced scope of any future Code of Practice) and the fact that these operators are already subject to security duty under the Communications Act we do not expect the TSR to have an impact on the number of these operators.

Will the TSR limit the ability of suppliers to compete or compete vigorously

8.9. By raising the security bar, this legislation should increase the demand for those vendors that place a high value on security and disincentivise the use of those vendors who do not.

8.10. However, the requirements will provide a ‘floor’ not a ‘ceiling’; operators will be encouraged to exceed them and constantly innovate to enhance security.

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

8.12. The Review found that there are a lack of commercial drivers for operators 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 operators are not currently competing on security features of their networks; and that the standardisation of security is unlikely to affect levels of competition.

Will the TSR limit the choices and information available to consumers

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

8.14. We expect that the TSR 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. Operators could use the TSR to communicate with their customers that they comply with a security standard. The fact that the TSR is standardised will allow consumers to understand better the way in which operators approach security and how important it is for the security and resilience of the service they receive.

Overview

8.15. Given that we do not find that this legislation will have any of the competition impacts highlighted in the CMA assessment we have not carried out a formal competition assessment.

9. A summary of the potential trade implications of measure

9.1. Operators who are subject to Telecoms Security legislation may seek to use vendors 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.

9.2. The NCSC's guidance, which is expected to form the technical backbone of the Code of Practice for the Telecoms Security legislation, currently includes requirements that relate to 'Retaining National Resilience and Capability'. It intends to mitigate the risk to the availability of both an operator's network and national networks in the event of disruption to international connectivity or in the event of disruption of offshore technical and operational support.

9.3. The NCSC sets out the intent of this requirement as:

> 'The intent of the TSRs 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 TSRs 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, from damaging UK networks.'[95]

9.4. This aspect of the guidance could affect inward investment flows where global operators are required to alter processes or move functionality to the UK, if it is included in the final Code of Practice.

9.5. This does impose an additional obligation on foreign businesses where management functionality is not currently in the UK, or those global operators headquartered in the UK who nevertheless may have some security functions or critical support based overseas. Impacts may be more limited for the majority of UK network operators.

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

10. Monitoring and Evaluation

How is the current system monitored

10.1. Ofcom has the following powers with respect to monitoring communications providers under the current system:

- Ofcom may require a network or service provider 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 Act to investigate, rectify, and penalise any infringement of these obligations.

10.2. In addition communications providers have a statutory obligation to report to Ofcom breaches of security or reductions in availability which have a significant impact on the network or service.

10.3. Ofcom's powers - which cover information gathering, audit, and investigation - derive from the need to ensure that operators have 'appropriate measures' in place. These powers are not designed to allow Ofcom to ensure compliance through continual monitoring of measures adopted by providers. Furthermore, Ofcom's functions are to oversee individual operators, rather than industry as a whole.

10.4. The guidance that is currently published by Ofcom to guide communications providers on their security and resilience obligations under sections 105A and 105B of the Communications Act 2003 (CA2003) has been updated once since its publication in May 2011.[96]

10.5. With reference to the updated guidance Ofcom note 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.'[97]

What external factors will impact on the success of the Telecoms Security legislation

10.6. The Telecoms Security legislation 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.

10.7. The most significant cyber threat to the UK telecoms sector comes from states. The UK Government has publicly attributed malicious cyber activity against the UK to Russia and China as well as North Korea and Iranian actors – and each have intentionally inflicted damage on the UK through cyber means. As set out in the

[96] 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.

[97] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance

previous section, the move to 5G brings a new dimension to the security risks, given the greater dependence that wider UK CNI is likely to have on UK telecoms than is the case with 3G/4G.

10.8. 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.’[98]

How will the Telecoms Security legislation be monitored

10.9. The Telecoms Security legislation will include a set of security duties and a Code(s) of Practice.

10.10. The frequency of reviews will need to ensure a balance is struck between the need to protect against new threats and account for technology changes, and the need to allow operators to focus on implementing a baseline security standard across the relevant areas of their networks and businesses.

10.11. When changes to the Code of Practice are made an implementation period will be allowed and this will be set out in the published guidance.

10.12. Ofcom will be required to regularly report to the Government on cross industry compliance with the security duties, having reference to the Code of Practice. This will provide information on the effectiveness of the regime.

10.13. Further to this, the NCSC’s continued monitoring of security threats and risk assessments, will provide a picture of the effectiveness of the regime. DCMS will consult with NCSC on the evolution of the Code of Practice.

10.14. A Post Implementation Review will take place by 01/01/2026.

[98] The Review, page 24.