

Title: The Telecommunications Security Bill 2020: National security powers in relation to high risk vendors IA No: RPC Reference No: Lead department or agency: Department for Digital, Media, Culture and Sport Other departments or agencies:	Impact Assessment (IA)
	Date: 21 May 2020
	Stage: Final
	Source of intervention: UK government
	Type of measure: Primary Legislation
	Contact for enquiries: Essie Barnett (essie.barnett@dcms.gov.uk)

Summary: Intervention and Options	RPC Opinion: Fit for purpose
--	-------------------------------------

Cost of Preferred (or more likely) Option (in 2019 prices)			
Total Net Present Social Value	Business Net Present Value	Net cost to business per year	Business Impact Target Status
-£1,578.9m	-£1,569.5m	£182.3m	£911.7m

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?

The cyber security risks can largely be managed and mitigated through technical measures, with the exception of the national dependence risk, where it is necessary for government to have the national security powers to intervene to set the conditions necessary, including by imposing limits and controls on the use of high risk vendors, so that operators can manage the risk.

To manage and mitigate the risk of national dependence on a vendor that is high risk, the national security powers relating to high risk vendors that will be introduced through the Telecoms Security Bill will provide the Secretary of State with the power to impose a range of limits and controls on the use of high risk vendors in UK telecoms networks.

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

The management of high risk vendors has, to date, relied on a mixture of formal cyber security mitigation arrangements (such as the long standing Huawei Cyber Security Evaluation Centre), administrative agreements and advice issued by the National Cyber Security Centre (e.g. under section 3(1)(b) Intelligence Services Act 1994). These informal arrangements, which represent the 'do nothing' option, are no longer sufficient in light of the fact that the next generation of mobile and fixed networks create new security and resilience challenges:

- 5Gs technical characteristics create a greater surface for potential attack;
- The speed, scale and processing power of these new technologies will enable a wide range of new services bringing a new dimension to the security risks and greater dependency that UK critical national infrastructure will have on telecoms; and
- These new technologies face an increasingly hostile threat environment.

In the absence of legislation, that advisory position continues in relation to the outcomes of the Supply Chain Review with advice published by the National Cyber Security Centre on the use of high risk vendors in the UK telecoms network. The advisory nature of the position means that it is not enforceable. UK Telecoms Operators can therefore choose to ignore the advice. That is insufficient reassurance to manage what is a national security risk to the UK Telecoms network.

The Review considered two options:

1. Exclude high risk vendors from the core of the network and restrict in the access network. This builds on the long-standing advice from the NCSC in relation to the core¹ of the network and adds restrictions in the access network to manage the national security risk of national dependence. Recommended option.
2. Exclude high risk vendors from the core of the network and the access network. This goes beyond the NCSC advice. Not recommended.

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: 17 August 2020

¹ The core includes critical telecoms network functions, such as user authentication and call routing.

Summary: Analysis & Evidence

Policy Option 1

Description: Exclusion of high risk vendors from core network functions and restrict their presence in the access networks, alongside exclusions from sensitive geographic locations.

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	PV Base Year 2020	Time Period 10 Years	Net Benefit (Present Value (PV)) (£m)		
			Low: -1,863.9	High: -1,533.0	Best Estimate: -1,578.9

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	1,665.4	0.8	1,533.0
High	1,995.6	1.3	1,863.9
Best Estimate	1,710.5	1.1	1,578.9

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

The monetised costs include the costs to operators of the following requirements (all costs in PV terms):

- Restrictions on high risk vendors in the Access network - £1,497m
- Exclusion of high risk vendors in the Core network - £72m
- Familiarisation costs - £0.2m

Additionally, Ofcom and DCMS will incur monitoring costs of £7-12m.

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

- Vendor oversight costs incurred by operators to provide ongoing support for the high risk vendor mitigation strategy

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0	0	0
High	0	0	0
Best Estimate	0	0	0

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

We have monetised the benefits of:

- Unlocking 5G use cases that would not have otherwise been unlocked as they are reliant on highly secure and resilient networks
- Reducing dependence on high risk vendors in the UK 5G and FTTP networks, saving costs in the event of needing to remove high risk vendor equipment from the network entirely

Whilst we have been able to monetise some benefits there remains uncertainty as to how much of these benefits can be attributed to the national security power. For that reason, we have not presented a figure for total benefits - instead we set out a breakeven analysis in the section [Direct costs and benefits to business calculations](#). **This analysis finds that if 12% of these benefits can be attributed to option 1 those benefits will offset the costs.**

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

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

We have made proxy estimates based on the available data. The costs to businesses quantified in the impact assessment are mainly equipment costs but we have not estimated other costs such as the cost of re-planning the network or the cost of running new procurement exercises which are likely to be small in comparison. We assume businesses are able to fund the additional costs without impacting other aspects of their operation resulting in indirect costs. We have not quantified the impact of any delay in rollout of 5G and Full Fibre networks. Lastly, we do not estimate impacts on international trade in quantitative terms as we have not identified substantial impact on total trade or investment flows.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs: 182.3	Benefits: 0	Net: 182.3183.2	
			911.7

Summary: Analysis & Evidence

Policy Option 2

Description: Exclusion of high risk vendors from both the core and access networks for full fibre and 5G.

FULL ECONOMIC ASSESSMENT

Price Base Year 2019	PV Base Year 2020	Time Period 10 Years	Net Benefit (Present Value (PV)) (£m)		
			Low: -2,201.8	High: -2,050.1	Best Estimate: -2,096.0

COSTS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	2,120.4	0.8	2,050.1
High	2,265.6	1.3	2,201.8
Best Estimate	2,165.5	1.1	2,096.0

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

The monetised costs include the costs to operators to 'rip and replace' high risk vendor equipment to meet the following requirements (all costs in PV terms):

- Core and Access Exclusion on high risk vendors in 5G and FTTP networks - £2,014m
- Exclusion of high risk vendors from certain network functions - £72m
- Familiarisation costs - £0.2m

Additionally, Ofcom will incur monitoring costs of £7-12m.

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

- Delay to roll out of 5G mobile full fibre fixed access networks

BENEFITS (£m)	Total Transition (Constant Price) Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0	0	0
High	0	0	0
Best Estimate	0	0	0

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

We have monetised the following benefits:

- Unlocking 5G use cases that would not have otherwise been unlocked as they are reliant on highly secure and resilient networks
- Reducing dependence on HRVs in the UK 5G and FTTP networks, saving costs in the event of needing to remove HRV equipment from the network entirely

Whilst we have been able to monetise some benefits there remains uncertainty as to how much of these benefits can be attributed to the national security power. For that reason, we have not presented a figure for total benefits - instead we set out a breakeven analysis in the section [Direct costs and benefits to business calculations](#). **This analysis finds that if 16% of these benefits can be attributed to option 2 those benefits will offset the costs.**

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

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

We have made proxy estimates based on the available data (eg data on global telecoms market). The costs to businesses quantified in the impact assessment are mainly equipment costs but we have not estimated other costs such as the cost of re-planning the network or the cost of running new procurement exercises which are likely to be small in comparison. We assume businesses are able to fund the additional costs without impacting other aspects of their operation resulting in indirect costs. We have not quantified the impact of any delay in rollout of 5G and Full Fibre networks. Lastly, we do not estimate impacts on international trade in quantitative terms as we have not identified substantial impact on total trade or investment flows.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs: 242.4	Benefits: 0	Net: 242.4	
			1212.1

Summary: Intervention and Options	1
Summary: Analysis & Evidence Policy Option 1	3
Summary: Analysis & Evidence Policy Option 2	5
Key terms	10
Problem under consideration and rationale for intervention	11
What is the issue being addressed	11
What are the current or future harms being tackled?	14
What sectors/markets/stakeholders will be affected?	16
Why is the government best placed to resolve the issue?	17
Rationale and evidence to justify the level of analysis	18
The Telecoms Supply Chain Review	18
Assessment and updating of advice on use of Huawei following US Sanctions	20
Description of options considered	22
The ‘Do nothing option’ or ‘Business as Usual’	22
What options have been considered?	23
Policy objective	25
Preferred policy option	26
How will the preferred option be given effect	26
Process for the assessment of vendors	26
Determining the controls on high risk vendors	27
Monetised and non-monetised costs and benefits of each option	30
The costs and benefits of the proposed approach	30
What is the counterfactual	31
Economic impact - costs	33
Number and type of businesses affected	33
What are the costs of Option 1?	34
Familiarisation costs	41
Monitoring costs	44
Vendor oversight costs	46
What are the costs of Option 2?	46
Other costs under Option 2	48
Economic Impact - benefits	48
Supply chain risks in the UK Telecoms Sector	49
Cyber attacks in the UK Telecommunications sector	50
High risk vendors in the UK Telecoms Sector	52
Economic benefits of 5G and Full Fibre	53
The Telecommunications Security Bill will unlock 5G use cases that would not have been deployed under a lower level of security	53
Sensitivity analysis and benefits illustration	59

The national security power will reduce the potential cost of dependence on a high risk vendor	59
Direct costs and benefits to business calculations	61
Breakeven analysis	64
Impact on small and micro businesses	66
Into what sector and/or subsector the affected businesses fall	66
Number of businesses in scope of the regulation	66
Impact on businesses (do these impacts fall disproportionately on small and micro business?)	68
Could SMBs be exempted while achieving the policy objectives?	70
Could the impact on SMBs be mitigated while achieving the policy objectives?	71
Competition impacts	73
What are the product and geographic markets?	73
Establishing the baseline	73
Will the measure directly limit the number or range of suppliers?	74
What is the impact of limiting the number of suppliers?	75
Will reduced numbers of suppliers affect prices?	75
What is the impact on prices in Access networks	76
The Core Exclusion will reduce the number of suppliers in the Core markets	77
Text redacted	78
Will the measures restrict choices for operators?	78
Impact on innovation	79
Quantified impacts Access Networks	79
Quantified Impacts Core	80
A summary of the potential trade implications of measure	81
Potential impacts on imports or exports	81
Direct or indirect impact on the value of overall trade or investment flows	81
Different requirements for domestic and foreign businesses?	82
The Basis of Different treatment	82
Monitoring and Evaluation	84
How is the current system monitored	84
What external factors will impact on the success of the national security power	84
How will the national security powers in relation to high risk vendors be monitored	85

Key terms

Term:	Referred to as:
The Telecoms Supply Chain Review	The Review
The Telecommunications Security Bill 2020	The Bill
National security powers in relation to high risk vendors	The national security power
Exclude high risk vendors from the core of the network	The Core Exclusion
Restrict high risk vendors in the access network	The Access Restriction
Exclude high risk vendors from the access network	The Access Exclusion
Exclude high risk vendors from both the core and the access networks	The Core and Access Exclusion
The NCSC's advice on the use of equipment from high risk vendors in UK telecoms networks	The NCSC guidance

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.

5G and full fibre networks must be secure and resilient

- 1.3. The deployment of 5G and full fibre networks across the UK is a primary objective of Government policy. The Government's 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.
- 1.4. 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.
- 1.5. These are set out in Box 1 which is an extract from the Review³:

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

² [UK Telecoms Supply Chain Review Report](#) (The Review), paragraph 1.3.

³ The Review, paragraphs 2.11 - 2.15.

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.

- 1.6. Likewise, increasing reliance on 'fibre to the premise' (FTTP) will make the security and resilience of these networks important.
- 1.7. This is explained in Box 2 which is an extract from the Review⁴:

Box 2: Increasing reliance on FTTP will make the security and resilience of these networks important

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

⁴ The Review, Paragraphs 2.19 - 2.22.

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 engineers visits and new customer premise equipment.

- 1.8. 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.
- 1.9. 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 highlighted the importance of network resilience as more businesses and individuals rely on over the top services⁵ to stay connected. This focus demonstrates 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

- 1.10. 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,

⁵ Over the top (or OTT) services is the term used to describe when a provider delivers audio, video and other media over an IP network. Apple's FaceTime, Google Hangouts, Skype and WhatsApp are examples of OTT services.

- 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.⁶
- 1.11. 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:

Negative 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 security compared to other factors such as cost and quality⁷. The same is true of businesses: the Cyber Breach Survey 2020⁸ found that only 15% of all businesses surveyed have reviewed the cyber security risks presented by their suppliers.

- 1.12. 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?

- 1.13. The UK's National Cyber Security Centre (NCSC) provided the expert technical cyber security analysis to inform the Review. This considered the threats and risks to the UK telecoms sector.

⁶ The Review, Paragraph 1.13.

⁷ 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.

⁸ [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.

- 1.14. The Review set out a telecoms sector threat assessment and the non-classified element of this assessment is reproduced in Box 3⁹.
- 1.15. It also identified four key risks associated with the telecoms supply chain:
- National dependence on any one vendor, especially ones deemed high risk;
 - Faults or vulnerabilities in network equipment;
 - The ‘backdoor’ threat – the embedding of malign functionality in vendor equipment; and
 - Vendor administrative access to provide equipment support or as part of a managed services contract.

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.

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

⁹ The Review, paragraphs 3.2 - 3.8.

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 testing¹⁰ 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).

11

- 1.16. Findings from the UK Cyber Breaches Survey 2020¹² 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.
- 1.17. 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 [7.54](#) of this report.

What sectors/markets/stakeholders will be affected?

- 1.18. The current regulatory framework for telecoms security is set out in the Communications Act 2003 (CA 2003) sections 105A to 105D. This framework is regulated by Ofcom which regulates compliance ex post through monitoring reports of breaches and auditing a network or service providers security measures where necessary as well as enforcement. This framework requires telecoms operators to be responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks.
- 1.19. The Telecoms Security Bill will look to enhance this framework, to level up security across the industry.

¹⁰ 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.

¹¹ Connected Nations 2018, Ofcom, December 2018

<https://www.ofcom.org.uk/research-and-data/multisector-research/infrastructure-research/connected-nations-2018/main-report>

¹² [Cyber Security Breaches Survey 2020: Statistical Release](#)

- 1.20. The current obligations set out in sections 105A - 105D of the Communications Act apply to all providers of Public Electronic Communications Networks (PECN) and Public Electronic Communications Services (PECS).¹³
- 1.21. The national security power relating to high risk vendors, will be broad in scope (applying to all public communications providers including all PECN and PECS and associated facilities), but the SoS will have the discretion to specify the application of the Direction within the Direction. The Secretary of State will set out controls by issuing a Direction to operators. Directions could be issued to either individual operators, or to groups of operators, falling within the scope of the proposed powers (i.e. any public communications provider).
- 1.22. In addition to the operators affected, the Government - including Department for Digital, Culture, Media and Sport (DCMS), and the NCSC - and Ofcom will be affected.

Why is the government best placed to resolve the issue?

- 1.23. The responsibility for the management of security and resilience risks to UK telecoms is shared between the Government, Ofcom and industry. Section [What sectors/markets/stakeholders will be affected?](#) set out that industry is currently responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks
- 1.24. 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.
- 1.25. Section [What are the current or future harms being tackled?](#) sets out the four risks that were identified in the telecoms supply chain. 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.

¹³ Section 105A to D of the Communications Act 2003 refers to network providers (providers of a public electronic communications network (PECN)) and service providers (providers of a public electronic communications service (PECS)). The Communications Act includes a wider definition of public communications providers the scope of which includes PECN, PECS and also associated facilities which are facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service.

2. Rationale and evidence to justify the level of analysis

The Telecoms Supply Chain Review

- 2.1. The Telecoms Supply Chain Review provided an evidence-based assessment of the telecoms supply chain, taking account of security, quality of service, economic and strategic factors.
- 2.2. GCHQ's National Cyber Security Centre (NCSC) provided DCMS with detailed security analysis and advice on the cyber security risks facing 5G and full fibre networks to underpin the Review. The NCSC is the UK's technical authority on cyber security. It is part of the NCSC's role to highlight potential cyber security risks to the UK's national security and provide advice based on their technical expertise.
- 2.3. The NCSC analysed the potential risk to the telecoms sector arising out of changes within the telecoms supply chain, the existing security practices employed by UK operators, and the residual risks to the UK.
- 2.4. The Review appointed KPMG as independent consultants to undertake economic analysis of the telecoms supply chain.
- 2.5. 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.
- 2.6. Officials carrying out the Review wrote to the major telecoms operators¹⁴ and suppliers¹⁵ 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 GSMA¹⁶, ETSI¹⁷ and 3GPP¹⁸) and the Emergency Services Network (ESN).
- 2.7. 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.
- 2.8. 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.

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).

- 2.9. The Review looked at the potential costs of controls on high risk vendors including an exclusion of high risk vendors from the core of the network and a restriction in the access network. To estimate these potential costs, information was gathered on each cost driver.
- 2.10. For 5G, the main cost drivers identified were:
- The need for mobile network operators (MNOs) to 'rip and replace' high risk vendor equipment from existing 4G mobile masts before they can be upgraded to 5G using equipment from an alternative supplier. This swap out is required due to a lack of interoperability between 4G and 5G equipment provided by different suppliers.
 - Higher equipment prices for future build as a result of reduced competition between equipment suppliers (due to constrained supply from high risk vendors).
 - The write off and replacement of high risk vendor 5G equipment already deployed.
- 2.11. For full fibre, the Review also considered operators could face higher equipment costs for new builds. However, 'rip and replace' costs were not applicable to full fibre networks as there are no interoperability issues with legacy equipment.
- 2.12. DCMS collected information on these costs as part of the Review and this information is used in this impact assessment. In a number of cases the information that DCMS collected was commercially confidential. Where DCMS has used this data to inform the analysis within this impact assessment we have not been able to set out in detail the sources of our assumptions in order to preserve the confidentiality of the data. Where this is the case we have set this out. Where additional information was required to assess impacts not assessed during the Review, we have estimated these based on available information.
- 2.13. DCMS published the Review in July 2019, setting out the key proposals for a new telecoms security framework. This would be centred on new telecoms security requirements (TSR) to indicate to industry what good security looked like. It would be underpinned by an enhanced legal framework under new legislation. The Review made conclusions and set out how the Government would take these forward, rather than being published as a consultation.
- 2.14. The Review's final conclusions - in January 2020 - followed a decision by the National Security Council and set out the need for new national security powers in relation to the presence of high risk vendors in UK networks, which would be taken forward in legislation. On 28 January, the NCSC published technical advice to operators in respect of their use of equipment from high risk vendors.¹⁹
- 2.15. The Government is now taking forward the recommendations of the Review. This is 'Phase 2' identified by the Telecoms Supply Chain Review, which was expected to lead to the:
- TSR being underpinned by new legislation, a statutory obligation on operators to comply with the new requirements and Ofcom given stronger powers to allow for the effective and enduring enforcement of the TSR.

¹⁹ NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, 2020.

- A new national security Direction power for the Secretary of State to require, as a last resort, operators to comply with specific controls in relation to individual high risk vendors and do other specified things that are reasonably necessary to protect networks from national security risks; and a new information obligation on operators to provide the Government with information about vendor arrangements that could raise national security risks.

Assessment and updating of advice on use of Huawei following US Sanctions

- 2.16. The Government made it clear in January that the NCSC would continue to review and update its advice as necessary.
- 2.17. On 15th of May, the US Department of Commerce announced that new sanctions had been imposed against Huawei through changes to the foreign direct product rules.
- 2.18. Although the sanctions were not the first attempt by the US Government to restrict Huawei's ability to supply equipment to 5G networks, they were the first to have potentially severe impacts on Huawei's ability to supply new equipment in the UK. The new US measures restrict Huawei's ability to produce essential components using US technology or software.
- 2.19. The NCSC reviewed the consequences of the US's actions, and reported to Ministers that they had significantly changed their security assessment of Huawei's presence in the UK 5G network.
- 2.20. The NCSC concluded that given the uncertainty the US sanctions created around Huawei's supply chain, the UK could no longer be confident it would be able to guarantee the security of future Huawei 5G equipment affected by the change in the US foreign direct product rules. To manage this risk, the NCSC issued new advice to the Government on the use of Huawei in UK telecoms networks.
- 2.21. On the morning of 15 July, the Prime Minister chaired a meeting of the National Security Council, during which attendees considered the NCSC's new advice, together with the implications for UK industry and wider geostrategic considerations.
- 2.22. The Government agreed with the NCSC's advice that to secure the UK's telecoms networks operators should stop using new affected Huawei equipment to build the UK's future 5G networks.
- 2.23. Consequently, on the afternoon of 15 July it announced that telecoms operators must stop purchasing affected 5G equipment from Huawei after 31 December 2020. It also announced that all Huawei equipment should be removed from 5G networks by the end of 2027. The existing ban on Huawei from the most sensitive 'core' parts of the 5G network, announced in January, would remain in place.
- 2.24. Government advised full fibre operators to transition away from purchasing new Huawei equipment. A technical consultation²⁰ would determine the precise timetable from which point fixed operators should stop procuring affected Huawei equipment.

²⁰ The consultation is being planned for the autumn.

2.25. Since the US sanctions impacted future Huawei equipment, the Government suggested there was no security justification for the removal of 2G, 3G or 4G equipment that is already in place. Instead, existing security mitigation arrangements for 2G, 3G and 4G should remain in place and the Government would continue to work with operators to mitigate risks, as it had been doing for some time.

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 and provision of guidance by the NCSC.
- 3.2. The existing security requirements under the Communications Act are set out in section [Box 4 - How does Ofcom regulate operators today?](#)
- 3.3. In addition to these requirements, historically, the involvement of high risk vendors has been managed on an advisory basis by NCSC, through advice provided to operators. In particular, when operators have approached NCSC about the use of HRVs, NCSC has advised them how best to mitigate the particular risks that they might present.
- 3.4. In addition, the NCSC operates a bespoke mitigation strategy for Huawei, which involves the operation of the Huawei Cyber Security Evaluation Centre (HCSEC).
- 3.5. NCSC have now published their high risk vendor guidance because the Government and NCSC recognise that the market is now at a crucial stage in new 5G and Fibre to the Premises (FTTP) rollout programmes and that industry urgently requires security advice now to support these programmes. This guidance is important in enabling operators to make security choices that will help to protect the security of their own, and the UK's, telecoms networks.
- 3.6. 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:
- 3.7. 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.²¹
- 3.8. These reasons underlie the risks of the do nothing option. If existing incentives are not sufficient for operators to address security failures the level of network security will be too low increasing the risk of cyber attacks on those networks.
- 3.9. If how to achieve the right level of network security is made clear to operators, for example through the NCSC guidance, they could find it easier to address security failures.
- 3.10. However, the Government does not believe that this guidance is sufficient to address the security concerns that have been raised by NCSC. And it has always been the Government's intention to seek further statutory powers in relation to the use of high risk vendors.
- 3.11. This has been considered in the context of the previous advice that NCSC has provided to operators and the efficacy of the HCSEC. The last two annual reports of the HCSEC Oversight Board highlighted serious cyber security and engineering flaws in Huawei products currently deployed in the UK.²²

What options have been considered?

- 3.12. Government has considered a range of policy options to address the issues identified by the Review in respect of High Risk Vendors. A number of potential options were identified by the Review to mitigate the risks presented by HRVs (either individually or in combination). These were:
- *Certification schemes*: Certification schemes usually work to ensure compliance with international standards. Certification schemes assume that a vendor is not hostile (i.e. they presume that the vendor is providing the 'real' source code or documentation). In this case, our assumption is that high risk vendors could be actively hostile, thus breaking the premise of a certification scheme.
 - *Bespoke vendor mitigation strategies*: The current bespoke mitigation strategy in place for Huawei, led by the NCSC, involves the operation of the HCSEC. The last two annual reports of the HCSEC Oversight Board highlighted serious cyber security and engineering flaws in Huawei products currently deployed in the UK.
 - *Deployment restrictions and exclusions on HRVs*: The Review considered two different possible approaches of this kind: exclusions (e.g. from particular network components or more widely), and/or restrictions (e.g. on a vendor's market share and/or on deployment in strategic locations). The level of intervention should be proportionate to the security risks identified across different network components. Security risks should also be considered in conjunction with the risks of economic dependency on high risk vendors across network components.

²¹ The Review, Paragraph 1.13.

²² <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019>

- 3.13. Of these three options it was concluded that whilst certification schemes may work to establish a baseline for all vendors, for high risk vendors we require a more targeted approach. Likewise, whilst bespoke vendor mitigation strategies should continue, they were not deemed to be sufficient.
- 3.14. As a result DCMS concluded that there was also a requirement for deployment restrictions and exclusions. Two options were considered in terms of deployment restrictions and exclusions.

Option 1: Core Exclusion and Access Restriction (preferred)

- 3.15. The Government's preferred option is exclusion of high risk vendors from core network functions and restriction of their presence in the access networks via a c.35% restriction alongside exclusions from sensitive geographic locations.²³
- 3.16. This option would combine imposing controls against the use of HRV products in the core of the network (i.e. the most safety critical part), with recommended restrictions on use of high risk vendor equipment in the access networks.
- 3.17. Operators must stop purchasing any new 5G equipment from Huawei after 31 December 2020 and all Huawei equipment should be removed from 5G networks by the end of 2027.

Option 2: Core and Access Exclusion

- 3.18. Exclusions of high risk vendors from both the core and access networks for full fibre and 5G.
- 3.19. This would involve imposing controls on UK telecoms operators not to use any high risk vendor manufactured equipment in their core and access networks for 5G and full fibre services.
- 3.20. Operators must stop using Huawei equipment for new build of both 5G and full fibre networks and remove any Huawei equipment already deployed within 2 years.

²³ Baroness Morgan's Oral Statement on UK Telecommunications, 28 January 2020
<https://www.gov.uk/government/speeches/baroness-morgans-oral-statement-on-uk-telecommunications>

4. Policy objective

- 4.1. The objective of the Bill is to protect the security of UK telecoms networks by enabling the Government to place legally binding controls on telecoms operators' use of high risk vendors within those networks.
- 4.2. The Government has ambitions to have the majority of the population covered by a 5G signal by 2027, with 15 million more premises connected to full fibre by 2025, and nationwide full fibre coverage by 2033. 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.
- 4.3. The NCSC currently provides advice to operators on the risks presented by high risk vendors and on the measure that the NCSC recommends they adopt as a result.²⁴
- 4.4. However, the Government does not currently have the power to impose binding controls on telecoms operators' use of high risk vendors. The Bill is intended to introduce such a national security power, enabling the Government to place controls, including limits, on operators' use of high risk vendors within their networks. It will also introduce requirements on operators to comply with those controls and sanctions for non-compliance.

²⁴ GCHQ has powers under section 3(1)(b) of the Intelligence Services Act 1994 to advise telecoms operators (and indeed the general public) about matters relating to the protection of information and other material. That has been used to provide advice on the risks posed by particular vendors and the appropriate mitigation measures.

5. Preferred policy option

How will the preferred option be given effect

- 5.1. The national security power should 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 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.

Process for the assessment of vendors

- 5.2. The Secretary of State will be responsible for making national security judgements and decisions in relation to potential high risk vendors, advised by the NCSC. Vendors will need to be designated in order for the national security direction powers to have their intended effect. Designation will allow the Secretary of State to place controls on operator use of high risk vendors that are already in the UK market or considering entering it (either to enable the Secretary of State to stop the company entering the market, or place appropriate conditions on entering the market).
- 5.3. A 'high risk vendor' is a vendor which poses an unacceptable risk, or risks, to the security and resilience of the UK's 5G and full fibre networks, and one that the Secretary of State may conclude – having regard to the available evidence – that it is necessary and proportionate to apply controls on telecoms operators in relation to the use of equipment from such vendors.
- 5.4. In determining whether a vendor presents an unacceptable risk, or risks, to the security and resilience of UK telecoms networks, the Secretary of State will have regard to a number of factors. These may vary over time, as the Government's understanding of the market, the supply chain and the threat environment evolves, but will likely include:
 - the key risks within the UK telecoms supply chain, as identified by the NCSC; and
 - any vendor-specific factors.
- 5.5. In response to the Telecoms Supply Chain Review, a non-exhaustive list of vendor-specific factors has been developed to aid the Secretary of State's decision on whether or not a vendor should be considered as high risk following a security assessment by the NCSC. The set of factors that have been used to make the recent judgements include:
 - the strategic position or scale of the vendor in the UK network;

- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market;
 - the quality and transparency of the vendor's engineering practices and cyber security controls;
 - the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;
 - the vendor's domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law;
 - the relationship between the vendor and the vendor's domestic state apparatus; and
 - the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.
- 5.6. This is intentionally a non-exhaustive list. Designation decisions will be based on the most appropriate and relevant set of factors allowing flexibility for changes in our understanding. To aid decision making there may be other relevant factors to take into consideration, such as the past behaviour and practices of the vendor and other factors relating to the ownership and operating location of the vendor.
- 5.7. The Secretary of State will keep under review the decision concerning which companies are classified as high risk, in light of the changing threat and technology landscape. As part of that process, it should be possible for companies 'designated' as high risk to draw the attention of the Government to any changes to their structure, technology or security practices that may impact the Government's risk assessment.

Determining the controls on high risk vendors

- 5.8. Having determined that a vendor is high risk, the Secretary of State will need to determine what controls will be required in order to manage the threat to national security from the potential use of such a vendor in the UK's telecoms networks.
- 5.9. In considering what controls to put in place, the Secretary of State will be informed by NCSC advice. The Secretary of State may seek to impose a range of different controls on the use of a high risk vendor(s) in UK telecoms networks. Before taking a decision on the appropriate controls to put in place, the Secretary of State will liaise with the NCSC to confirm whether an NCSC-approved mitigation strategy is in place or could be put in place for any given high risk vendor.
- 5.10. The following list details the types of controls the Secretary of State may seek to impose on operators:
- Limiting the use of high risk vendors in certain network functions by imposing a specified restriction on the use of a network equipment type;
 - Prohibiting the use of high risk vendors in certain network functions;

- Prohibiting the use of high risk vendors across an entire network²⁵;
- Prohibiting the use of high risk vendors in certain locations;
- Prohibiting the use of more than one high risk vendor in any given network.

Establishing controls on the use of high risk vendors

- 5.11. The Secretary of State will set out controls by issuing directions to operators. Directions should be issued to either individual operators, or to groups of operators, falling within scope of the proposed powers (i.e. that being any public communications providers.²⁶
- 5.12. A direction from the Secretary of State will set out a range of details necessary for the direction to have effect. This will include details such as the operator(s) it applies to; the vendor(s) it relates to; a summary assessment of the vendor against relevant vendor designation criteria; the controls that should be put in place in relation to the vendor(s) specified; the date by which the controls must be implemented by the operator(s); any evidence expected to be provided by operators for the purposes of assessing compliance with any controls specified in the direction, and the frequency with which that evidence should be provided to the Secretary of State; specify Ofcom's role (if any) in monitoring compliance with the direction; highlight that non-compliance with a direction would be considered unlawful and that sanctions could be imposed for non-compliance.
- 5.13. It is expected that in the majority of cases the issuing of a direction should be public. The Secretary of State will take all reasonable efforts to issue a public direction. There may be some cases where the public issuing of a direction in and of itself poses a threat to national security. In those rare cases it may be necessary to issue a classified direction.
- 5.14. The ability for the Secretary of State to issue a direction to operators in relation to the limits and controls necessary on the use of high risk vendors will reflect one or a selection of the types of controls envisaged. As the threats and risks change, so too may the types of controls that it may be possible, or appropriate, to impose on the use of designated high risk vendors so it will be important that the ability to impose limits and controls is flexible enough to respond to potential different future scenarios.
- 5.15. As part of the new framework created by the Telecoms Security Bill, any directions issued by the Secretary of State will take precedence over any requirements placed on operators as part of the Telecoms Security Requirements. However, the expectation is that they should be complementary arrangements.

²⁵ In the case where a high risk vendor does not have an NCSC-approved mitigation strategy, the Secretary of State may choose to implement a complete exclusion on operator use of such a vendor.

²⁶ Section 151 of the [Communications Act 2003](#) defines a public communications provider.

Requiring operators to provide information relating to vendor arrangements

- 5.16. The Secretary of State will need to be provided with accurate information from UK telecoms operators on their vendor arrangements to make decisions on:
- the designation of high risk vendors, and
 - operator compliance with controls set out in directions.
- 5.17. The information required will likely include:
- information on the current use of potential high risk vendors in the operators network;
 - information on the current use of designated high risk vendors in the operators' network;
 - information on the use of new vendors, not previously used in the UK network, that may be considered for a new procurement contract, and that will need to be assessed in order to determine whether they may be high risk; and
 - wider information on network details to facilitate the application and assessment of compliance with controls set out in directions.
- 5.18. The Secretary of State may contact any public communications provider to request such information. The Secretary of State will determine within what timeframe such information should be submitted, and the frequency with which such information should continue to be submitted where requested.

6. Monetised and non-monetised costs and benefits of each option

- 6.1. This impact assessment makes an estimation of the costs and benefits of the options under consideration where possible. While this impact assessment brings together evidence from a number of sources, we would like to note there are still a number of limitations to the analysis.
- Due to a lack of robust and specific data, for example on UK telecoms market size and the size of specific sub-markets, we have made proxy estimates based on the available data (eg data on global telecoms market).
 - The costs to businesses quantified in the impact assessment are mainly equipment cost (such as the cost of new equipment and price increases) and associated costs where available (such as the cost of replacing the equipment) but not other potential costs (such as the cost of re-planning the network or the cost of running new procurement exercises) which are likely to be small in comparison; given the size of the equipment costs and that these are administrative costs that may only need to be brought forward rather than requiring additional costs.
 - We assume businesses are able to fund the additional costs without impacting other aspects of their operation resulting in indirect costs as expenditure on equipment is a relatively low proportion of their overall expenditure.
 - We have not quantified the impact of a delay in rollout of 5G and Full Fibre networks on public communications providers.
- 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 national security powers relating to high risk vendors 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 national security powers relating to high risk vendors 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 national security powers relating to high risk vendors.

The costs and benefits of the proposed approach

- 6.4. The types of controls the Secretary of State may seek to impose on operators as set out in the section [Summary and preferred option with description of implementation plan](#) above are:
- Limiting the use of high risk vendors in certain network functions by imposing a specified restriction on the use of a network equipment type (the Access Restriction);
 - Prohibiting the use of high risk vendors in certain network functions (the Core Exclusion);

- Prohibiting the use of high risk vendors across an entire network²⁷;
 - Prohibiting the use of high risk vendors in certain locations (the Geographic restrictions);
 - Prohibiting the use of more than one high risk vendor in any given network.
- 6.5. In the Review the NCSC assessed that these policies (Option 1) offer the optimal solution from a cyber security perspective.
- 6.6. In addition to the cyber security conclusions, the Review also considered the economic impact of both the preferred policy options and alternate options.
- 6.7. The Review considered two options:
- Option 1 (preferred): the exclusion of high risk vendors from core network functions and restriction of their presence in the access networks alongside exclusions from sensitive geographic locations (i.e. 'Core Exclusion and Access Restriction').
 - Option 2: the exclusions of high risk vendors from both the core and access networks for full fibre and 5G (i.e. 'a Core and Access Exclusion').
- 6.8. The Review found that either of the two options would have economic impacts, including:
- on telecoms operators in the form of deployment delays and increased costs, and
 - on high risk vendors, depending on their presence (and aspired to presence) in the UK.
- 6.9. The economic impact of a 'Core and Access Exclusion' would be greater than a 'Core Exclusion and Access Restriction' approach.
- 6.10. In addition to these impacts DCMS has considered the measures announced in July - which require that telecoms operators must stop purchasing any new Huawei 5G equipment after 31 December 2020 and that all Huawei equipment should be removed from 5G networks by the end of 2027.
- 6.11. These measures are within the scope of Option 1 which restricts the use of high risk vendors in the Access networks. The incremental impacts of the July measures increase the impact of Option 1 by extending the Access restriction but the costs of Option 1 continue to be lower than Option 2.

What is the counterfactual

- 6.12. In the section [Description of options considered](#) we set out the 'do nothing' option. This 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.
 - The publication of non-binding NCSC guidance on the use of HRV operators in UK 5G and full fibre networks.

²⁷ In the case where a high risk vendor does not have an NCSC-approved mitigation strategy, the Secretary of State may choose to implement a complete exclusion on operator use of such a vendor.

- 6.13. Under this 'do nothing' option the counterfactual for our analysis are the current rollout plans and vendor landscape that operators had in place at the time of the Review. This is the best information that we have as to how these markets would have evolved without intervention. Whilst it is possible that operators may have changed these plans as a result of NCSC guidance without this legislation we do not have enough information to assess whether this is the case. As a result our estimates may be conservative - they may overstate the costs if some of these costs would have been incurred anyway as operators adjust their plans to take account of NCSC guidance.
- 6.14. We also note that on 15th of May, the US Department of Commerce announced that new sanctions had been imposed against Huawei through changes to the foreign direct product rules which have potentially severe impacts on Huawei's ability to supply new equipment in the UK. The NCSC concluded that given the uncertainty the US sanctions created around Huawei's supply chain, the UK could no longer be confident it would be able to guarantee the security of future Huawei 5G equipment affected by the change in the US foreign direct product rules. To manage this risk, the NCSC issued new advice to the Government on the use of Huawei in UK telecoms networks including that NCSC's Huawei mitigation strategy would exclude certain products including post sanction 5G equipment.²⁸
- 6.15. It is possible that this action would have an impact on our counterfactual which is based on information received at the time of the Review. If operators would have reduced their reliance on Huawei absent Government intervention this would mean that our estimates are, again, conservative. However, we don't have any information on how the sanctions would have affected rollout plans absent intervention. We therefore do not update our counterfactual to reflect this.
- 6.16. Whilst both Huawei and ZTE have been assessed to be high risk, only Huawei has a significant UK market presence. None of the other companies with a significant UK market presence are currently assessed as high risk.
- 6.17. Huawei is the leader in 4G radio access networks in the UK with a market share of c.35%²⁹ overall. Its market share in full fibre access networks is c.45%,³⁰ albeit full fibre connections are at a low level today (c.10% of total UK households). Additionally, Huawei has a presence in core networks. Its market share across the UK fixed and mobile core and transport sectors is estimated to be 15%.³¹
- 6.18. Whilst this is the current vendor landscape in the UK we also consider as relevant in our assessment the global vendor landscape (discussed in section [Exclusion of HRV equipment from the Core](#) below).

²⁸ [NCSC advice on high risk vendors in UK telecoms](#), July 2020.

²⁹ The Review, Paragraph 4.7

³⁰ Ibid

³¹ <https://www.endersanalysis.com/reports/huawei-and-5g-identifying-risks>

Economic impact - costs

- 6.19. For the purposes of this impact assessment we have updated the analysis undertaken for the Review to include an assessment of the preferred policy option (option 1). We assess the impact of the Secretary of State issuing a number of Directions within the scope of Option 1. Directions can be issued under the national security power which provides the Secretary of State with the ability to issue directions to telecoms operators placing controls on the use of equipment from high risk vendors. The Directions we assess would entail the exclusion of high risk vendors from core network functions and restriction of their presence in the access networks, alongside exclusions from sensitive geographic locations and option 2 which sets out a Core and Access Exclusion.
- 6.20. We also consider familiarisation costs, monitoring costs and vendor oversight costs.

Number and type of businesses affected

- 6.21. The scope of the Review was PECS and PECN - this shaped the engagement and the policy recommendations made in the Review - including the recommendation for a power to allow the Secretary of State to impose operator controls on the use of HRVs. The Communications Act includes PECN and PECS in the definition of public communications providers, the scope of which also includes associated facilities. These are facilities which are essential in the provision of an electronic communication network or service, or support the provision of 'other services' provided by means of that network or service. Examples include telephone calls completed through interactive voice response boxes, TV transmission with MPEG compression supported by compression systems and email supported by e-mail servers³².
- 6.22. The power to impose high risk vendor controls should be able to be exercised in relation to all public communications providers as defined in the Communications Act.³³ As set out in section [Preferred policy option](#) the Secretary of State will set out controls by issuing directions to operators. Directions should be issued to either individual operators, or to groups of operators, falling within scope of the proposed powers (i.e. that being any public communications provider).³⁴
- 6.23. Therefore, for the purposes of this Impact Assessment, we assume that all public communications providers could be subject to the proposed powers in relation to high risk vendors.
- 6.24. We set out available information on the number of public communications providers below:

³² https://www.ofcom.org.uk/_data/assets/pdf_file/0021/46434/guidelines.pdf

³³ It should not directly apply to equipment vendors or managed service providers, though these entities will be impacted through the new requirements on network operators. Operators who provide bespoke private networks to business customers would not be included in this definition.

³⁴ Section 151 of the [Communications Act 2003](#) defines a public communications provider.

- Public communications providers who currently pay Administrative fees to Ofcom and therefore have a relevant turnover of over £5m. There were 119 such operators in 2019/20³⁵
 - Public communications providers who have applied for Code Powers under the Electronic Communications Code and are therefore on Ofcom's 'Register of persons with powers under the Electronic Communications Code'. There were 176 such companies on 3rd March 2020.³⁶
 - All other public communications providers who have a relevant turnover of under £5m and do not have code powers. We refer to these companies as the 'long tail' and we do not know how many there are. 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).
- 6.25. The national security powers in relations to high risk vendors will not directly apply to equipment vendors, though these entities will be impacted through the new requirements on network operators. We do not estimate costs for these companies as these costs will be ultimately paid by public communications providers who use the services that these companies provide.

What are the costs of Option 1?

The Restriction in the Access network

- 6.26. As part of the Review we considered the costs of a restriction on high risk vendor equipment in the access network and a exclusion in the core network. We briefly set out the types of costs assessed for each option here before setting out the costs in more detail below.
- 6.27. For 5G, the Review found that the main types of costs are:
- The need for MNOs to 'rip and replace' Huawei equipment from existing 4G mobile masts before they can be upgraded to 5G using equipment from an alternative supplier. This swap out is required due to a lack of interoperability between 4G and 5G equipment provided by different suppliers.
 - Higher equipment prices for future build as a result of reduced competition between equipment suppliers (due to constrained supply from Huawei).
- 6.28. We also expect some operators will incur costs in write off and replacement of Huawei equipment already deployed.³⁷ This is as a result of the Government's

³⁵ 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

³⁶ 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, <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>

³⁷ The written off cost of Huawei equipment already deployed is not included in the cost estimates which are for the replacement costs of new equipment.

announcement on 15th July that all Huawei equipment should be removed from 5G networks by the end of 2027.

6.29. We estimated these costs using a model which is described in Box 4 below.

Box 4: Access networks cost models

The estimates of the cost impacts of the Restriction in the access networks is based on modelling developed during the Review, separately for mobile (5G) and fixed (FTTP) networks.

For 5G networks, the model considers the four UK mobile network operators active in the UK. For each operator, we use an estimate of the number of masts they use, the proportion of masts with high risk vendor equipment, and the proportion of masts expected to be upgraded to 5G by 2025, to quantify the number of masts operators expect to upgrade using high risk vendor equipment in the counterfactual.³⁸

We quantify three types of costs.

1. For the high risk vendor masts not yet upgraded to 5G, we quantify the cost of removing 4G high risk vendor equipment already installed³⁹ and replacing it with equipment from another vendor. We also quantify the incremental cost of upgrading to 5G using a non-high risk vendor (allowing for the difference in baseline cost).
2. For the high risk vendor masts already upgraded to 5G, we quantify the cost of removing 4G high risk vendor equipment already installed and replacing it with equipment from another vendor, and the full cost of 5G equipment from a non-high risk vendor. We depreciate these costs on a straight-line basis taking into account the expected lifetime of the equipment and the removal timetable.
3. For all masts (both already upgraded and to be upgraded to 5G), we quantify the impact of higher prices due to reduced competition.⁴⁰

For FTTP networks, the model considers the main FTTP infrastructure provider (Openreach) and the many alternative providers (Altnets) in aggregate. For Openreach and the aggregated Altnets, we use an estimate of the number of premises that they currently cover and expect to cover with FTTP by 2025, and the proportion of premises (expected to be) covered using high risk vendor equipment, to quantify the number of premises operators expect to cover using high risk vendor equipment in the counterfactual.⁴¹

³⁸ Estimates are based on engagement with industry and analysis produced by external consultants for DCMS as part of the Telecoms Supply Chain Review.

³⁹ Based on the cost of the relevant equipment.

⁴⁰ Estimates are based on engagement with industry and analysis produced by external consultants for DCMS as part of the Telecoms Supply Chain Review.

⁴¹ Ibid

We quantify two types of costs. For the premises expected to be covered using high risk vendor equipment, we quantify the incremental cost of doing so using a non-high risk vendor (allowing for the difference in baseline cost). For all premises, we quantify the impact of higher prices due to reduced competition.⁴²

- 6.30. For full fibre, operators 'rip and replace' costs are not applicable as there are no interoperability issues with legacy equipment. However, as with 5G there are costs as a result of higher equipment prices.
- 6.31. For the purposes of this impact assessment we have included all of these costs. Which are, in summary:
- estimates of rip and replace costs for Mobile Access markets;
 - removal of installed 5G equipment including higher equipment prices for replacement equipment; and
 - higher prices for future build of mobile and fixed networks (price impacts are discussed in section [Wider impacts](#) below).⁴³

Equipment costs: Rip and replace costs

[Redacted]

[Redacted]

		[Redacted]
[Redacted]	■	■
[Redacted]		■
[Redacted]	■	■
[Redacted]	■	■

[Redacted]

[Redacted]

		[Redacted]
[Redacted]	■	■

⁴² Ibid

[Redacted]

[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		[REDACTED]
[REDACTED]		

Impact on rollout

- 6.38. We expect that the restriction will affect operators' roll out plans for both 5G and full fibre networks as they divert engineering resources and capital expenditure from 5G and FTTP build. In total the restriction on the procurement of new Huawei 5G equipment from the end of this year will delay rollout by a further year (in addition to a delay of a year as result of the Access restriction announced in January 2020). In addition, requiring operators to remove Huawei equipment from their 5G networks by 2027 will further delay roll out. This means a cumulative delay to 5G rollout of two to three years. For full fibre networks we assume a shorter delay of around 1 year reflecting the transition period for the restriction on deployment of new Huawei equipment.
- 6.39. We have not estimated any direct costs to business of this roll out delay. Whilst we expect that operators will incur costs undertaking network replanning exercises

and running new procurement processes, these costs will be small in relation to the overall equipment costs.

Restrictions on Geographic Areas

- 6.40. In its guidance on the use of High Risk Vendors the NCSC set out controls on the use of HRV in access networks near certain sites that are significant to national security. We call these the Geographic Restrictions.
- 6.41. These sites are not listed but the NCSC has set out that it has already provided advice to many affected operators, and any others who think their networks may be affected should consult NCSC.
- 6.42. Whilst we do not know how many sites will be affected yet we have made some assumptions based on the key risks that the geographic restrictions seek to address. [REDACTED]
- 6.43. Based on these characteristics, we expect that the total number of sites will be low [REDACTED]. We also note that this equipment would also be affected by the restriction on the purchase of Huawei equipment from 2021 and the timetable for the removal of Huawei equipment from our 5G network by 2027. We therefore expect that the Geographic Restrictions would not have a significant impact on costs, at worst bringing forward costs that would be incurred under other requirements. We therefore do not quantify these costs.

The Exclusion of HRV equipment from the Core

- 6.44. We assume that - as a result of the Exclusion- operators will remove HRV equipment from their networks by 2023 as per the NCSC's guidance (see below on [time period](#)) and replace it with alternative equipment from other (non-HRV) vendors. We use the value of this installed equipment to estimate the costs of the replacement equipment. This is a proxy and it assumes that there is no (material) difference in the value of the equipment and no (material) costs of switching equipment.
- 6.45. Industry estimates suggest Huawei had a share of around 15% in the fixed and mobile core networks⁴⁴, based on the number of subscribers. NCSC have proposed guidance that would require operators not to use equipment from High Risk Vendors in core networks, which would result in this share to fall to zero.
- 6.46. The proportion of Huawei equipment in the core is low in the UK by international standards and industry estimates suggest that the average share of Huawei equipment in mobile core networks globally is circa 25%, with ZTE having a further 10% share⁴⁵. We assume that there is a similar share in the global fixed core networks⁴⁶. The relatively low share in the UK may reflect the impact of longstanding guidance by the NCSC which indicated that Huawei equipment

⁴⁴ Enders Analysis's 'Huawei and 5G: Identifying the risks', 8th March 2019 - figure 5

⁴⁵ <https://www.fiercewireless.com/tech/ericsson-holds-slight-lead-over-huawei-mobile-core-market>

⁴⁶ Across the whole telecoms equipment market globally, Huawei has a share of 28% and ZTE has a share of 10%. This is similar to the mobile core network share so we assume the fixed core network also has a similar share. <https://www.delloro.com/the-telecom-equipment-market-2019/>

should not be used in the core. NCSC set this out in their current advice on the use of equipment from high risk vendors in UK telecoms networks:

“In order to minimise the additional cyber security risk caused by HRVs, NCSC believe it is necessary and proportionate to limit their presence in networks. This has been NCSC’s consistent advice to operators (when they have sought our guidance) and is most operators’ existing common practice; that advice is now being formalised and published, as requested by Government. NCSC’s advice is that use of HRVs without these restrictions would cause a cyber security risk that cannot be effectively mitigated.”⁴⁷

6.47. NCSC has also issued guidance on the use of ZTE in telecommunications infrastructure:

“NCSC assess that the national security risks arising from the use of ZTE equipment or services within the context of the existing UK telecommunications infrastructure cannot be mitigated.”⁴⁸

6.48. We consider that the low proportion of Huawei equipment in the core could be a result of the ‘consistent advice’ given by NCSC. However, we also recognise that this could be a result of UK operator preferences. Therefore, we consider as a lower bound for our estimate the costs of removing high risk vendor equipment from the core based on existing UK market shares and an upper bound based on the global counterfactual.

6.49. The global mobile core network market value for the 12 months ending in the third quarter of 2019 is estimated at \$7.5bn (a 14% increase on the previous year, giving an estimate for the global mobile core network market value in 2018 at \$6.6bn).⁴⁹ The UK mobile core network market is estimated to be \$105-150m for that year (using the assumption that in the total mobile market, the UK is 1.4-2.0% of the global market⁵⁰).

6.50. The UK Fixed Core Network market value is estimated to be \$75-110m for the same period using the assumption that the UK fixed core network market is c.70% of the UK mobile core network market, in line with the proportion for the global mobile and fixed equipment/services markets^{51,52,53}.

6.51. The NCSC guidance sets out a time period for operators to remove Huawei equipment from the specified network functions:

⁴⁷ <https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks>

⁴⁸

<https://www.ncsc.gov.uk/news/zte-ncsc-advice-select-telecommunications-operators-national-security-concerns-0>

⁴⁹ <https://www.fiercewireless.com/tech/ericsson-holds-slight-lead-over-huawei-mobile-core-market>

⁵⁰ Based on industry returns to the Telecoms Supply Chain Review.

⁵¹ This is derived from global fixed equipment/services market size divided by global mobile equipment/services market size <https://www.delloro.com/the-telecom-equipment-services-market-forecast/>

⁵² Given the uncertainty in this percentage from using global numbers, we have used a range of c.50%-90% for the low and high scenarios in table 4.

⁵³ By estimating the fixed core network market value from our mobile core estimate, all assumptions we have made for the UK mobile core network market value have also been assumed for the fixed core network market value.

‘From a cyber security perspective, the NCSC advises operators whose Huawei estates currently exceed the recommended level for an HRV, to reduce to the recommended level as soon as practical. We understand that this takes time, but consider that it should be possible for all operators to reduce their use of HRVs to the recommended levels within 3 years.’⁵⁴

- 6.52. This would mean that operators should comply with the advice by 28th Jan 2023. We have used this timeframe for the purposes of this impact assessment.
- 6.53. Given this advice has been widely publicised and shared with operators, we assume that operators would not install HRV equipment in their core networks after the date that NCSC published their guidance (January 2020).⁵⁵ This assumption means that operators would avoid some of the costs of removing equipment as a result of the implementation period proposed by the NCSC. As such the proposed implementation period provides a mitigation of the impacts of the policy and therefore the costs that operators avoid are considered a result of the overall policy and not included in the EANDCB calculator.
- 6.54. Based on information received during the Review we also assume that equipment in the core has a replacement cycle of 3-5 years in both the mobile and fixed core⁵⁶. Given the timing of the Exclusion and the replacement cycle of equipment, we would expect only HRV equipment installed during 2018 and 2019 would be present in operators' networks once the Exclusion comes into force in 2023. The proportion of equipment installed during these years will depend on each operator's procurement and installation schedule. For simplicity, we assume that on average operators install equipment at an even pace.

Table 4: Estimate of HRV equipment in UK Core Networks in 2023

		Low	High	Best estimate ⁵⁷
Estimated size of UK Core Network market (years 2018 and 2019) ⁵⁸	£m ⁵⁹	230	415	315

⁵⁴

<https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks>

⁵⁵ Both EE and Vodafone have publicly stated that they plan to remove Huawei equipment from their core networks.

⁵⁶ The information we received related to the replacement cycle for mobile networks. We assume this is also the case for the fixed core network.

⁵⁷ For our best estimate we use the midpoint of our assumptions for the estimated UK core network market and the proportion of this market supplied by HRVs under the counterfactual scenario.

⁵⁸ Calculated by adding the estimates for the UK fixed core network market value and the UK mobile core network market value in 2019 (as above) to estimates for both market values in 2018 (calculated with the same methodology as for 2019, but with a global mobile core network value of \$6.6bn instead of \$7.5bn). This has then been converted to pounds.

⁵⁹ Market size converted from dollars to pounds using the exchange rate on 28th January 2020; \$1=£0.77

Proportion of Core Network market supplied by HRVs under counterfactual scenario	%	15 ⁶⁰	35 ⁶¹	25
Value of HRV equipment in UK Core Networks (purchased in 2018 and 2019)*	£m	30	150	75
NPV over impact assessment period	£m	29	145	72

Note: Results are rounded to £5m pa.

Familiarisation costs

- 6.55. We consider familiarisation costs for each option compared to Business As Usual. Business as Usual refers to continuing with the existing security requirements under the Communications Act 2003 and provision of guidance by the NCSC.
- 6.56. We note that operators may incur two types of familiarisation costs;
- Reading and understanding the legislation and
 - Reading and understanding any subsequent Directions issued.
- 6.57. In January 2020 the Government announced it's clear intention to legislate seeking additional powers to enforce compliance on telecoms operators' use of high risk vendors within the UK telecoms network'.⁶²
- 6.58. This announcement was followed by the publication of NCSC guidance which hoped to assist the market by making a clear statement of advice setting out how the presence of a particular vendor may increase security risks, what a high risk vendor is and how to manage the particular security risks presented by those vendors.⁶³
- 6.59. This guidance is relatively brief and has been publicised widely since its publication. The issue of use of high risk vendors has also been widely discussed by industry. We therefore expect that under the Business as Usual scenario the vast majority of operators will be familiar with the principles of the powers the Government is seeking and the NCSC guidance - which sets out the detail of how these powers might be applied.
- 6.60. However, when the Government introduces legislation creating national security powers in relation to high risk vendors we expect that all affected businesses will seek to understand the specific impact of those powers on their business. Initially we expect this would require a legal professional to read and understand the legislation and that would include reading the legislation and explanatory notes and drafting a summary of the legislation. Our legal department have estimated that this would require approximately three hours from a legal professional.

⁶⁰ Huawei market share in the UK core and transport network market in 2018; Enders Analysis's 'Huawei and 5G: Identifying the risks', 8th March 2019 - figure 5

⁶¹ Huawei and ZTE combined market share in the global mobile core network in 2019;

<https://www.fiercewireless.com/tech/ericsson-holds-slight-lead-over-huawei-mobile-core-market>

⁶² <https://www.gov.uk/government/speeches/jeremy-wrights-oral-statement-on-the-telecoms-supply-chain-review>

⁶³ This advice is in addition to NCSC's historic management of high risk vendor use on an advisory basis by NCSC, through advice provided to operators. Furthermore, NCSC has encouraged operators who are considering introducing new vendors into their networks to discuss this with them.

- 6.61. As discussed [above](#), given the level of familiarity that we expect most operators will have with NCSC guidance on high risk vendors we estimate that dissemination costs will be limited to updating the Executive team on the contents of the legislation and disseminating relevant information to procurement teams as required. We estimate that this could require approximately 10 hours across a mix of staff members which we approximate as IT specialist managers (see [Table 5 below](#)).
- 6.62. However, operators who are issued a Direction - under the powers the Government is seeking - will incur further familiarisation costs as they read and understand the detail of the Direction.
- 6.63. A Direction will set out a range of details necessary for the direction to have effect. This will include details such as the operator(s) it applies to; the vendor(s) it relates to; a summary assessment of the vendor against relevant vendor designation criteria; the controls that should be put in place in relation to the vendor(s) specified; the date by which the controls must be implemented by the operator(s); any evidence expected to be provided by operators for the purposes of assessing compliance with any controls specified in the direction, and the frequency with which that evidence should be provided to the Secretary of State; specify Ofcom's role (if any) in monitoring compliance with the direction; highlight that non-compliance with a direction would be considered unlawful and that sanctions could be imposed for non-compliance.
- 6.64. As a Direction has not yet been issued we cannot directly estimate familiarisation costs. To give an indication of the scale of costs we assume that, initially, the Secretary of State issues Directions affecting 10 operators and that each Direction sets out the details described above. Based on guidance from our legal team we expect the time required for a legal professional to read and understand a Direction would be substantially more and a communications provider would likely take in-depth legal advice, consult technical expertise in the business about the implications, and consider how to implement the direction. However, this would be offset to some degree by the familiarity of operators with the NCSC guidance and the legislation.
- 6.65. We estimate that for each Direction operators would incur 10 hours of familiarisation costs from a member of their legal department and approximately 10 hours from a mixture of staff across procurement and other functions required to understand the impact of a Direction on an operators network infrastructure. This does not include detailed planning or re-procurement costs which are outside the scope of familiarisation costs.

Estimating Familiarisation Costs

- 6.66. The wages for technology and telecommunications directors and legal professionals are taken from the ONS' Annual Survey of Hours and Earnings⁶⁴. The median is used as a best estimate, as it is believed to be the most representative wage (it is less skewed by outliers).

⁶⁴ ONS, Annual Survey of Hours and Earnings, Provisional - Occupation SOC 10 (4) Table 14.5a Hourly pay - Gross 2019.

Table 5: Wage per hour: Annual Survey of Hours and Earnings (2019)

Job Title	Hourly wage rate			Hours	Total wage cost (Median)	Uplift for overheads ⁶⁵
	Median	Low (20th percentile)	High (80th percentile)			
Familiarising with the legislation (all operators)						
IT specialist managers	36.55	26.63	48.6	10	£366	£447
Legal professional	39.57	25.62	58.94	3	£119	£145
Familiarising with a Direction (operators who receive a Direction)						
IT specialist managers	36.55	26.63	48.6	10	£366	£447
Legal professional	39.57	25.62	58.94	10	£396	£483

6.67. The 20th and 80th percentiles were chosen as high and low estimates. Overhead charges of 22% are added to the wages, in accordance with RPC guidance on implementation costs⁶⁶ which uses Eurostat data on UK non-wage and wage costs to calculate this uplift.

6.68. Based on this data our best estimate of familiarisation costs will be that all public communications providers with Code Powers will incur around £600 in familiarisation costs and those that are subject to a Direction will incur an additional £1,000 per Direction. Based on the number of businesses set out in the section [Number and type of businesses affected](#) we estimate familiarisation costs for public communications networks with Code Powers and for operators receiving a Direction:

- Around £600 per public electronic network with code powers. Based on 228 such operators, this would total around £140,000.
- Around £1,000 per Direction and per Operator. If 10 such Directions are issued, total familiarisation costs will be £10,000.

6.69. In addition to public communications providers with Code Powers there are also public communications providers without Code Powers.

⁶⁵ RPC_short_guidance_note_-_Implementation_costs__August_2019.

⁶⁶ RPC_short_guidance_note_-_Implementation_costs__August_2019.

- 6.70. Because there is inherent uncertainty about the number of public communications providers without Code Powers we provide an estimate in line with the impact on public electronic networks with Code Powers. We estimate that:
- if the total number of public electronic networks without Code Powers is twice the number of those with Code Powers but they incur half the level of familiarisation costs on average; they will incur the same level of familiarisation costs in total i.e. £140,000.
- 6.71. We note that the total familiarisation costs are small so the impact of this assumption on the total costs estimates will be negligible.

Monitoring costs

- 6.72. The compliance model for the proposed national security powers relating to high risk vendors is one whereby all national security judgements and decision-making, enforcement and sanction decisions are undertaken by the Secretary of State (as advised by the NCSC). In carrying out this role, the Secretary of State may be supported by Ofcom who may be asked to provide information relating to operator use of high risk vendor equipment, products and/or services.
- 6.73. This model entails similar monitoring costs both for operators and for Government / Ofcom. These are:
- Operators would be required to provide information on their use of high risk vendors. This would include:
 - the current use of potential high risk vendors in the operators network;
 - the use of designated high risk vendors in the operators' network and
 - the use of new vendors, not previously used in the UK network, that may be considered for a new procurement contract, and that will need to be assessed in order to determine whether they may be high risk.
 - operators networks more generally so as to ensure the controls set out are appropriate in each case
 - Government or Ofcom would be required to review and analyse the information provided on an on-going basis drawing on technical experts such as the NCSC to support an assessment of whether operators are complying with any specified controls.
 - Government or Ofcom would be required to provide a report to the Secretary of State setting out the level of compliance with the direction.
- 6.74. The costs would be driven by the number of High Risk Vendors identified, the number of controls for each vendor and the type and frequency of information required. There are five types of controls that the Secretary of State could impose:
- Limiting the use of high risk vendors in certain network functions by imposing a specified restriction on the use of a network equipment type;
 - Prohibiting the use of high risk vendors in certain network functions;

- Prohibiting the use of high risk vendors across an entire network⁶⁷;
- Prohibiting the use of high risk vendors in certain locations;
- Prohibiting the use of more than one high risk vendor in any given network.

6.75. It is expected that both Ofcom and DCMS will incur costs in carrying out these functions. We estimate these costs in table 6 below based on information provided by Ofcom and DCMS in May 2020. These estimates are based on a best guess of the future requirements for compliance with Option 1 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 HMT as Ofcom work towards approval of final required spend.

Table 6 - Costs of monitoring compliance with the national security power

	Costs of monitoring compliance with the national security power	
	Total costs in net present value terms over the period 2020 - 2029 (3.5% discount rate), £m	
	Low estimate	High estimate
Ofcom costs	5.4	8.9
DCMS costs	1.7	2.8
Total	7.0	11.7

6.76. Ofcom is expected to recover these costs through a negotiated rise in its spending cap via retention of the Wireless Telegraphy Act licence fees that Ofcom collects on behalf of HM Treasury.⁶⁸ DCMS are currently exploring this with HM Treasury and any increase will be agreed with DCMS and HM Treasury in line with Ofcom's statement of principles on Wireless Telegraphy Act retention⁶⁹.

6.77. We do not include these costs as a direct cost to business because they are a retention of funds which are collected on behalf of HM Treasury. There will be no charge applied directly to businesses for Ofcom's activities or any increase in charges already applied.

6.78. We do not have estimates of the costs to operators of providing information to Ofcom and DCMS and given the reporting requirements set out above we expect

⁶⁷ In the case where a high risk vendor does not have an NCSC-approved mitigation strategy, the Secretary of State may choose to implement a complete exclusion on operator use of such a vendor.

⁶⁸ Under the Communications Act 2003, certain fees, charges and penalties which Ofcom receives from stakeholders must be paid into the government's Consolidated Fund. Ofcom may, however, make a statement setting out the principles under which it may retain amounts in order to fund its spectrum management work and to meet certain costs which it cannot otherwise recover through imposing fees and charges.

⁶⁹ Retention of Amounts paid under the Wireless Telegraphy Act 2006, 28th May 2020.

these to be small in proportion to total operator costs - for that reason we do not estimate them.

Vendor oversight costs

- 6.79. NCSC has in place a wider mitigation strategy for oversight of Huawei which includes the Huawei Cyber Security Evaluation Centre (HCSEC) which has been in place since 2010. The direct costs of HCSEC are borne by Huawei whilst the Government incurs costs of engagement with the HCSEC.
- 6.80. The NCSC noted that 'Before HCSEC was set up in 2010, similar work was being done but through a different mechanism'.⁷⁰ In this respect Huawei has always been treated as a 'high risk vendor' and their use in the UK has been limited with extra mitigations around their equipment and services.
- 6.81. In the case of Huawei, operators would be required to provide ongoing support for the NCSC approved Huawei mitigation strategy, which amongst other things comprises the Huawei Cyber Security Evaluation Centre. These costs, alongside the costs of running the Huawei Cyber Security Evaluation Centre are already incurred and this process has been in place since 2010.
- 6.82. Should further HRVs be identified further costs of oversight would be required.

What are the costs of Option 2?

The Exclusion in the Access network

- 6.83. A Core and Access Exclusion would entail the same types of costs to a Restriction which are set out in section [What are the costs of the Restriction in the Access network?](#). However, costs will be proportionally higher reflecting the fact that whilst the same number of sites are affected the exclusion would require operators to stop using Huawei equipment for new build sooner and remove any Huawei equipment already deployed within 2 years. Removing assets more quickly means that each asset has been depreciated less when it is removed meaning that the costs of removal are higher.

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

⁷⁰ <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Other costs under Option 2

- 6.87. Under Option 2 the costs of the [Exclusion of HRV equipment from the Core](#) will be incurred in the same way as under Option 1 and these costs are set out above.
- 6.88. Other costs - incurred under Option 1 - are likely to be similar under Option 2 but could be lower due to decreased complexity of a Core and Access Exclusion relative to a Core Exclusion and Access Restriction. These costs are:
 - [Familiarisation costs](#)
 - [Monitoring costs](#)
- 6.89. We do not have estimates for these costs under Option 2 so we take a conservative approach of assuming that they are the same as under Option 1. Given the size of these costs relative to the total costs of Option 1 and Option 2 this is a proportionate approach.

- 6.90. [Vendor oversight costs](#) would be avoided under Option 2. However, these costs are not quantified under Option 1.

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 and specifically the national security power. These benefits relate to both Option 1 and Option 2.
- 6.92. A 2018 Ericsson report⁷¹ found that the two main barriers to 5G deployment 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’⁷².
- 6.93. We consider the economic benefit arising from 5G use cases where network security and resilience are considered a prerequisite to their deployment are likely to be an economic benefit resulting from the Telecoms Security Bill and that the national security power will contribute to this benefit.
- 6.94. We also consider the impact of a reduced national dependence on high risk vendors by estimating the potential cost to operators of an unmanaged exit which requires operators to completely remove high risk vendor equipment from their Access network.
- 6.95. 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 national security power - we do not have any information on which to base such an assumption. Instead we present a breakeven analysis.

Supply chain risks in the UK Telecoms Sector

- 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 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’.⁷³
- 6.97. Security of 5G and full fibre networks is determined by a range of factors and the NCSC has set out five areas of high risk in it’s ‘Summary of the NCSC’s security analysis for the UK telecoms sector’⁷⁴. These areas include the supply chain and

⁷¹ Ericsson: The Industry Impact of 5G. January 2018

⁷² [5G Economy Global Public Survey Report Commissioned by Qualcomm](#)

⁷³ [UK Telecoms Supply Chain Review Report](#)

⁷⁴ Summary of the NCSC’s security analysis for the UK telecoms sector, <https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf>

Figure 1 below shows the breakdown of the supply chain risks that the NCSC identified.

Figure 1 - A breakdown of supply chain risk



Source: Summary of the NCSC's security analysis for the UK telecoms sector, Figure 5.5.1-1.

6.98. This diagram shows the ways in which a vendor can increase supply chain risk including: trojan threat; equipment quality; data; national dependence and supplier network access. These risks do not relate solely to high risk vendors but in the same report NCSC found that:

- There are issues with Huawei's engineering 'the 2018 and 2019 HCSEC Oversight Board reports highlighted serious quality and security issues with Huawei's engineering. While the NCSC does not believe that the issues are due to malicious intent, they increase the risk to the UK regardless.'⁷⁵
- With regard to equipment trojans; these risks are particularly exacerbated in the case of high risk vendors⁷⁶

Cyber attacks in the UK Telecommunications sector

6.99. 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 2020⁷⁷. The information and communications sector, in which the telecoms sector sits, 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

⁷⁵ *ibid*, Paragraph 5.5.4.

⁷⁶ *ibid*, Paragraph 7.5.1.

⁷⁷ [Cyber Security Breaches Survey 2020: Statistical Release](#), 2020

the last 12 months, compared to 46% across all UK sectors and 47% for the same sector last year.

- 6.100. 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.⁷⁸
- 6.101. 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 attack⁷⁹. This is higher than any other sector surveyed. For 42% of telecoms companies surveyed, attacks resulted in in-house application downtime, which caused poor customer experience online.
- 6.102. Recent case studies of attacks on telecommunications companies in the UK include the following:
1. 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.⁸⁰
 2. 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.⁸¹
 3. 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 occurred over 5 days, with no known cause or outcome.⁸² According to Dyn, the company that noted the incident, it was carried out by Vega, a Ukrainian internet service provider.⁸³
 4. 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 2016.⁸⁴
- 6.103. The O2 example serves to demonstrate that major network failures can arise from faults on the side of the equipment vendor.

⁷⁸ [DDoS Threats Report 2018 Q3](#), 2018

⁷⁹ <https://www.efficientip.com/wp-content/uploads/EfficientIP-2017-Report-DNS-Threat-Survey.pdf>, 2017

⁸⁰ https://www.theregister.co.uk/2018/12/06/ericsson_o2_telefonica_uk_outage/

⁸¹ <https://www.telegraph.co.uk/news/2018/11/19/talktalk-hackers-jailed-18-months-2015-cyber-attack-caused-misery/>

⁸² <https://arstechnica.com/information-technology/2015/03/mysterious-snafu-hijacks-uk-nukes-makers-traffic-through-ukraine/>

⁸³ <https://qz.com/364110/the-mysterious-internet-mishap-that-sent-data-for-the-uks-nuclear-program-to-ukraine/>

⁸⁴ Summary of the NCSC's security analysis for the UK telecoms sector, 2020, Paragraph 5.5.3.

High risk vendors in the UK Telecoms Sector

- 6.104. The NCSC defines high risk vendors as ‘vendors that pose a higher security risk to UK telecoms networks’⁸⁵. The NCSC has drawn up a list of criteria which it applies when identifying vendors as HRVs.⁸⁶
- 6.105. To illustrate some of the ways in which a high risk vendor may pose a higher security risk, we have included the list of reasons that the NCSC cites for considering Huawei an HRV⁸⁷:
1. Huawei has a significant market share in the UK already, which gives it a strategic significance;
 2. It is a Chinese company that could, under China’s National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
 3. We assess that the Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and our interests;
 4. Our experience has shown that Huawei’s cybersecurity and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns in 2018 about Huawei’s engineering processes. Its 2019 report confirmed that “no material progress” had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted “further significant technical issues” that had not previously been identified; and
 5. A large number of Huawei entities are currently included on the US Entity List. Although we do not have knowledge as to whether these entities will remain on the US Entity List, this listing may have a potential impact on the future availability and reliability of Huawei’s products.

⁸⁵ [NCSC advice on the use of equipment from high risk vendors in UK telecoms networks](#), 2020

⁸⁶ These non-exhaustive criteria are:

- a. The vendor’s strategic position/scale in the UK network;
- b. The vendor’s strategic position/scale in other telecoms networks, in particular if the vendor is new to the UK market;
- c. The quality and transparency of the vendor’s engineering practices and cyber security controls;
- d. The past behaviour and practices of the vendor;
- e. The vendor’s resilience both in technical terms and in relation to the continuity of supply to UK operators;
- f. A number of considerations relating to the ownership and operating location of the vendor, including:
 - i. The influence which the domestic state apparatus can exert on the vendor (both formal and informal);
 - ii. Whether the relevant domestic state and associated actors possess an offensive cyber capability that might be used to target UK interests;
 - iii. Whether a significant component of its business operation is subject to domestic security laws which allow for external direction in a manner that conflicts with UK law.

⁸⁷ [NCSC advice on the use of equipment from high risk vendors in UK telecoms networks](#), 2020

Economic benefits of 5G and Full Fibre

- 6.106. The deployment 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 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.’⁸⁸
- 6.107. Previous analysis undertaken by DCMS has quantified the estimated economic benefits of 5G and full fibre-to-the-premises broadband (FTTP) rollout over the next 8 years.⁸⁹ The model was built using five industry reports which estimate the economic benefits produced.⁹⁰ The key results are detailed below⁹¹.

Table 9: 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

- 6.108. The modelling shows a combined benefit of £461bn to the UK over the next 8 years. This is the total economic benefit generated by the deployment of 5G and full fibre.

The Telecommunications Security Bill will unlock 5G use cases that would not have been deployed under a lower level of security

- 6.109. This analysis of the benefits of the national security powers relating to high risk vendors makes the argument that the economic value generated by a number of 5G use cases are dependent on secure and resilient networks.

⁸⁸ [UK Telecoms Supply Chain Review Report](#), 2019

⁸⁹ 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.

⁹⁰ 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.

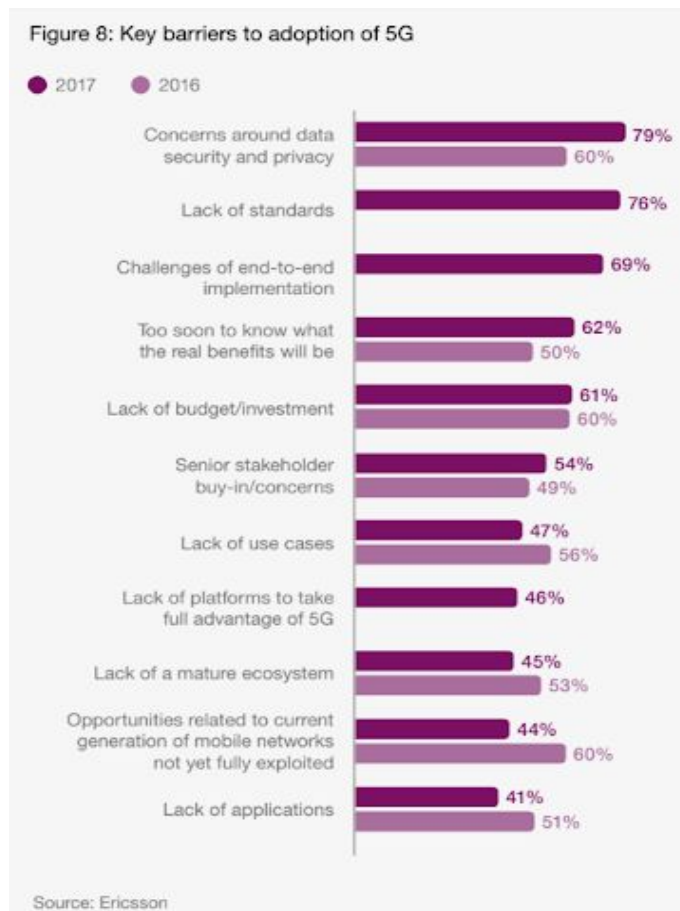
⁹¹ We have estimated the benefits to the UK economy from 5G and FTTP rollout based on available literature. Estimates of the economic benefits of 5G are uncertain at this stage. Our analysis of different sources suggests that potential benefits of 5G in 2025 could be around c.£25bn (with a range from 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).

- 6.110. From our literature review of twelve reports published over the last four 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.
- 6.111. 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.’⁹²
- 6.112. 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 report⁹³ that the two main barriers to 5G deployment are concerns around data security and privacy and lack of standards. This is demonstrated in Figure 2.

⁹² [How 5G Could Transform the Delivery of Healthcare](#)

⁹³ Ericsson: Industry Impact of 5G. January 2018.

Figure 2: Key barriers to adoption of 5G



- 6.113. The national security power will give the Government the power to issue a Direction to control the use of a high risk vendor(s) in UK telecoms networks. We are making the assumption that these powers - alongside the wider Telecoms Security Bill - will contribute to the unlocking of 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.
- 6.114. In order to quantify these benefits, we have looked at the economic benefit of four use cases. We have estimated the economic value of these cases, and then undertaken breakeven analysis to illustrate the size of these benefits relative to the costs of the national security powers.
- 6.115. The Ericsson report highlighted the four 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
- 6.116. 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 sectors⁹⁴. 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’. 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

6.117. 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 within the next 10 years in the table below.

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

Use case	Economic benefit (£bn)
Remote medical examination	3.1
Remote health monitoring	3.3
Autonomous cars	3.8
Total (2020-29)	10.2

6.118. The total monetisable benefits of the three identified use cases between 2020 and 2029 is estimated to be 10.2bn, in present value terms. This figure is based on estimated economic benefits and deployment timelines for each use case. We set out these estimates below:

Remote medical examination

6.119. 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 regulations⁹⁵

6.120. 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.’⁹⁶

⁹⁴ [5G Economy Global Public Survey Report Commissioned by Qualcomm](#)

⁹⁵ [Ericsson's 5G Business Potential report](#)

⁹⁶ [How 5G Could Transform the Delivery of Healthcare](#)

- 6.121. O2 published a report on the value of 5G in May 2018 ('the O2 report'), which estimates that high quality and secure tele-health video conferencing will allow people to conduct GP consultations from their smartphone or other smart devices. This will save individuals an estimated 3.3 hours per year, saving £1.3bn in lost productivity through workplace absence.⁹⁷ 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.'⁹⁸
- 6.122. Global Market Insights predict the use of telehealth will triple by 2025, fuelled largely by 5G⁹⁹. The same report states that the 'Teleconsultation service market is expected to grow at 18.9% CAGR across the forecast timeframe.'¹⁰⁰
- 6.123. 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. As detailed in the cost section, we have assumed a 3 year delay to the rollout of 5G such that in our model, the £1.3bn benefit is realised in 2028. 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 2027, we have assumed that the benefit will increase linearly from £0 in 2026 to £1.3bn in 2028. Beyond 2028, we have assumed the 18.9% CAGR growth rate reported above.

Remote health monitoring

- 6.124. 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.'¹⁰¹

- 6.125. 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

⁹⁷ [The value of 5G for cities and communities](#)

⁹⁸ [NHS Long Term Plan v1.2 August 2019](#)

⁹⁹ [Global Telemedicine Market size to exceed \\$130.5 Bn by 2025](#)

¹⁰⁰ [Telemedicine Market By Service Type, Component and Deployment | Forecast 2023](#)

¹⁰¹ [GSMA: Internet of Things in the 5G Era](#)

tracking possibilities, with enhancement in transmitting information between patients and health care services'.¹⁰²

- 6.126. The O2 report estimates that health monitoring devices will reduce 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 budgets¹⁰³. We have assumed that both use cases require secure and reliable networks, with a potential annual benefit of £1,353 million by 2025¹⁰⁴. 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.¹⁰⁵
- 6.127. 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 2022¹⁰⁶.
- 6.128. Our analysis of the economic benefits of remote medical monitoring starts with the £1.3bn benefit expected in 2025, based on the O2 report. As above, we have modelled the 3 year delay to 5G rollout so that the £1.3bn benefit is realised in 2028. 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

- 6.129. 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.'¹⁰⁷
- 6.130. 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 2030¹⁰⁸. 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.
- 6.131. 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

¹⁰² [Remote Patient Monitoring Within a Future 5G Infrastructure, Oleshchuk and Fensli, 2010](#)

¹⁰³ [The value of 5G for cities and communities](#)

¹⁰⁴ [The value of 5G for cities and communities](#)

¹⁰⁵ [The Growing Value of Digital Health in the United Kingdom](#)

¹⁰⁶ [Medtech and the Internet of Medical Things How connected medical devices are transforming health care](#)

¹⁰⁷ [10 things 5G can do that 4G can't](#)

¹⁰⁸ [Connected and Autonomous Vehicles – The UK Economic Opportunity](#)

track to meet its commitment to have fully self-driving vehicles on UK roads by 2021¹⁰⁹. However, Emerj, an AI research and advisory company, forecasts a different outcome.

- 6.132. 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.’¹¹⁰
- 6.133. Another government publication, Road Traffic Forecasts 2018¹¹¹, forecasted the years that different levels of connected and autonomous vehicles enter the market between the late 2020s and late 2040s.
- 6.134. 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. This is in line with the estimated 5G rollout date of 2028. 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

- 6.135. To ensure our analysis is robust, we have conducted some sensitivity analysis on these benefits. 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 £1.96bn.
- 6.136. Furthermore, not all of these benefits can be attributed to the Telecoms Security Bill. 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).

The national security power will reduce the potential cost of dependence on a high risk vendor

- 6.137. National dependence is one of the supply chain risks set out by the NCSC in its ‘Summary of the NCSC’s security analysis for the UK telecoms sector’¹¹². [Figure 1](#) which shows the NCSC’s breakdown of supply chain risks sets out the three potential impacts of national dependence which are: managed exit; influence and unmanaged exit.

¹⁰⁹ [Government moves forward on advanced trials for self-driving vehicles](#)

¹¹⁰ [The Self-Driving Car Timeline – Predictions from the Top 11 Global Automakers](#)

¹¹¹ [Road Traffic Forecasts 2018](#)

¹¹² [Summary of the NCSC's security analysis for the UK telecoms sector](#)

- 6.138. In this section we estimate the potential cost to operators of an unmanaged exit which requires operators to completely remove HRV kit from their Access network.
- 6.139. An unmanaged exit, could occur for a number of reasons, including:
1. Commercial failure of a vendor
 2. Imposition of sanctions
 3. Systemic faults in network equipment (intentional or unintentional)
 4. A security incident that raises additional concerns about HRV equipment
- 6.140. The higher the dependency on high risk vendors, the more likely the UK networks are to experience disruption due to such an event.
- 6.141. In order to estimate the costs associated with such a scenario, we have modelled a hypothetical event where UK telecommunications companies have to strip Huawei equipment out of their networks entirely. In this model, there are three scenarios:
1. The Counterfactual scenario: Operators have continued to roll out 5G and FTTP networks using Huawei equipment in the access networks in line with their original plans. This assumes no Huawei equipment is used in the Core network, as stated by several operators.
 2. Option 1: Operators have no Huawei equipment in the Core networks and have rolled out 5G and FTTP networks with a restricted Huawei presence in the access networks. By 2027, no Huawei equipment is used in the 5G network, but a limited amount of Full Fibre equipment is present.
 3. Option 2: Operators have no Huawei equipment in their 5G and FTTP networks.

We have used the Supply Chain Review model to estimate the costs of removing Huawei equipment under the counterfactual (£4.6bn), Option 1 (£0.4bn) and Option 2 (£0). [Box 4](#) describes how the model works and what information it uses to estimate these costs. There are no costs of removing equipment under Option 2 because under the Exclusion there is no HRV equipment in the networks.

- 6.142. In summary, the model estimates the costs of stripping out the Huawei equipment and replacing it with equipment from alternative suppliers. We assume that this is the case because, in practice, if a supplier failure occurs and there is no long-term maintenance option for the equipment already installed, operators would need to replace it. It is important to note that the cost of purchasing equivalent equipment from alternative suppliers is higher due to the price differential between Huawei and its competitors and the impact of reduced competition. The cost estimates for each scenario are below (not including write-off costs and rounded to the nearest £100m):

Table 11: Costs of unmanaged exit (in cash terms), to illustrate the benefit associated with reduced dependence on HRV

	Counterfactual	Option 1	Option 2
Removing Huawei equipment	£2.0bn	£0.1	£0
Purchasing alternative	£2.7bn	£0.3	£0

equipment			
Costs of unmanaged exit (cash terms)	£4.6bn	£0.4	£0
Benefits of reduced dependence (NPV)	n/a	£3.1bn	£3.4bn

Note: figures might not sum due to rounding.

- 6.143. The existence of the national security power means that the cost of such an event could be reduced by £4.2bn in cash terms (£4.6bn less £0.4bn) under Option 1 and £4.6bn under Option 2. As we want to illustrate the potential impact of a significant event, we have assumed that the replacement of the equipment takes place after the rollout of 5G and Full Fibre networks has completed in c.2028 (in line with the estimated delay to operator plans). This event could happen sooner, and if it were to take place during the rollout the impact would be lower.
- 6.144. Assuming the cost of replacing the equipment is borne in 2029 (after networks are assumed to be rolled out, and within the 10-year period of the impact assessment), the present value would be £3.1bn under Option 1 and £3.4bn under Option 2.

Direct costs and benefits to business calculations

- 6.145. Table 12 provides a summary of the costs that we have estimated. These include:
- the costs of excluding HRV equipment from the Core
 - the costs of rip and replace in 5G access networks
 - the costs of replacement equipment in 5G networks
 - the price impact on both 5G and full fibre access networks
- 6.146. The costs that we have estimated relate to the impact of controls the Secretary of State may seek to impose on operators. We have estimated the impacts where we expect these to give rise to a significant cost to business (the Restriction and the Exclusions). The costs we have estimated are:
- Limiting the use of high risk vendors in certain network functions by imposing a specified restriction on the use of a network equipment type (the Access Restriction);
 - Prohibiting the use of high risk vendors in certain network functions (the Core and Access Exclusions);
- 6.147. We have not estimated the cost of the following controls which we do not expect to give rise to a significant cost.
- Prohibiting the use of high risk vendors in certain locations (the Geographic restrictions).
 - Prohibiting the use of products and services from more than one high risk vendor in any given network
 - Prohibiting the use of high risk vendors across an entire network

The Geographic restrictions affect certain sites but given the impact of the Access Restriction we do not expect this to have significant incremental costs. The prohibition of more than one high risk vendor in a network relates to the use of ZTE in UK networks as at the present time only Huawei and ZTE have been assessed as HRVs by the NCSC.¹¹³ Given this, at the current time, the use of more than one high risk vendor would relate to the use of Huawei and ZTE equipment in any given network.

The case of prohibiting the use of an HRV across an entire network would apply where a high risk vendor does not have an NCSC-approved mitigation strategy, in which case the Secretary of State may choose to implement a complete exclusion on operator use of such a vendor. At the present time, whilst Huawei and ZTE have both been designated high risk vendors only Huawei has a mitigation strategy in place which includes the Huawei Cyber Security Evaluation Centre (HCSEC) which has been in place since 2010¹¹⁴.

NCSC have previously set out - in May 2018 - that use of ZTE equipment in UK telecommunications networks pose a risk that cannot be mitigated.¹¹⁵ We consider that, as a result of this advice and based on information received during the Review, the presence of ZTE in UK networks is limited and therefore the costs of these requirements are not significant.

Table 12: Summary of the estimated costs of the preferred policy option (excluding monitoring costs) - best estimate

Cost category	Total cash cost (£m)	Present value (£m)
Option 1		
Costs of excluding HRV equipment from the Core	75	72
Costs of the Restriction on HRV equipment in the Access network	1,635	1,497
Familiarisation cost	0.2	0.2
Total	1,710	1,570
Option 2		
Costs of excluding HRV equipment from the Core	75	72
Costs of excluding HRV equipment in the Access network	2,090	2,014
Familiarisation cost	0.2	0.2
Total	2,165	2,087

¹¹³ <https://www.ncsc.gov.uk/information/hrv-faq>

¹¹⁴ On 14th July 2020 NCSC set out that the Huawei mitigation strategy would exclude certain products as a result of impact of US sanctions. The impact of this exclusion is considered under Option 1.

¹¹⁵ <https://www.ncsc.gov.uk/news/zte-ncsc-advice-select-telecommunications-operators-national-security-concerns-0>

- 6.148. For Option 1 we assume that access equipment costs are incurred in the first 5 years of the impact assessment period, except the cost of replacing existing equipment which is spread over a longer period (until 2027). For Option 2, we estimate that all costs would be incurred in the transition period. For equipment costs this reflects the NCSC's advice that operators should look to implement its advice by January 2023. We expect price increases - set out in section [What is the impact on prices in Access networks](#) below - will persist until network roll outs are completed i.e mid-2020s. However, in our modelling we have assumed all costs are incurred in the implementation period. This reflects both a conservative approach of bringing costs forward¹¹⁶ and the fact that operators might agree prices and purchase equipment in advance of installing it.
- 6.149. These costs give a present value cost to business of approximately £1.6bn as our best estimate (with a range of £1.5 - £1.9bn) for Option 1 and £2.1bn (£2.0 - £2.2bn) for Option 2. In addition to these costs we estimate that monitoring costs create ongoing costs of £9.1m over the impact assessment period and additional transition costs of £0.3m (in present value terms) and that familiarisation creates one off costs of £0.2m.¹¹⁷
- 6.150. Whilst these are significant costs to industry the impact on consumer prices is likely to be low overall because active telecoms equipment represents a small proportion of the total operator cost base.
- 6.151. Any impact on consumer prices would be very hard to estimate, given operators face differential cost impacts, their individual competitive positions and commercial strategies, and the ability to bundle products with other offerings. We therefore do not present such an estimate.
- 6.152. There are significant benefits of the national security powers set out 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 dependence on HRVs in the UK 5G and FTTP networks
- 6.153. The most significant monetised benefit - 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 £10.2bn between 2020 and 2029, in present value terms. There are also potential benefits from avoiding dependence on a high risk vendor.
- 6.154. Whilst we have monetised these benefits we have not included them in the final calculation of net impact or EANDCB as doing so would require us to make an assumption about what proportion of benefits to attribute to the national security power. We do not have sufficient information to make this assumption. Instead we present a breakeven analysis below..

¹¹⁶ Bringing costs forward results in a higher NPV as the impact of discounting is reduced.

¹¹⁷ All figures rounded to the nearest £5m.

Breakeven analysis

- 6.155. The break-even point is the point at which total cost and total benefits are equal, i.e. "even". There is no net loss or gain. Breakeven analysis is a useful tool where total potential benefits are large but there is uncertainty about the degree to which these benefits can be attributed to the policy in question.
- 6.156. We include the following benefits we have identified in this analysis:
- Unlocking 5G use cases will create economic benefits some of which can be attributed to the Telecoms Security Bill including the national security power.
 - Reducing the potential cost of dependence on a high risk vendor: we estimated the cost of an event where high risk vendor equipment must be removed from UK networks.
- 6.157. In our breakeven analysis we calculated the proportion of the benefits relating to unlocking 5G use cases that we would need to attribute to the national security power in order to exceed the costs of implementing them. We found that, for Option 1, where the costs of implementing the national security power are approximately £1.6bn, the benefits would exceed the costs if we can attribute at least 16% of the total economic benefits of the 5G-enabled use cases to the power. This falls to 12% if we include the benefit of reducing dependence on a high risk vendor.
- 6.158. In the worst case - if costs are at the high end of our range and benefits at the low end¹¹⁸ - the potential total economic benefits of these 5G enabled use cases are approximately equal to the expected costs of Option 1.

Table 13 - Breakeven Analysis of Costs and Benefits (in present value terms)

	Costs of implementing national security power	Potential Benefits of unlocking 5G use cases	Potential Benefits of reduced impact of dependence on HRV	Breakeven Proportion of potential benefits
Option 1				
Breakeven against potential benefits of 5G use cases (central case)	£1.6bn	£10.2bn	N/A	16%
Breakeven against potential benefits of 5G use cases (worst case)	£1.9bn	£1.9bn	N/A	Costs and benefits approximately equal

¹¹⁸ Benefits at the low end refers to 5G enabled use cases delayed by two years and no benefits of reduced dependence on high risk vendors.

Breakeven of potential benefits of 5G use cases (central case) including potential benefits of reduced dependence	£1.6bn	£10.2bn	£3.1bn	12%
Option 2				
Breakeven against potential benefits of 5G use cases (central case)	£2.1bn	£10.2bn	N/A	20%
Breakeven against potential benefits of 5G use cases (worst case)	£2.2bn	£1.9bn	N/A	N/A (costs exceed benefits)
Breakeven of potential benefits of 5G use cases (central case) including potential benefits of reduced dependence	£2.1bn	£10.2bn	£3.4bn	16%

Note: Breakeven calculations based on rounded figures in for illustration.

We note that the break even analysis 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 £461bn¹¹⁹ to the UK over the next 8 years in Table 9 above. These wider benefits of the rollout of these networks may include additional use cases for which security and resilience are important which would indicate a set of much larger potential benefits. As such our break even analysis - with respect to the benefits of 5G use cases - should be considered an illustration of some of the benefits that we can monetise.

¹¹⁹ This benefit is based on five industry reports which estimate the economic benefits produced and does not take into account any delays to rollout of these networks as a result of either Option 1 or Option2.

7. Impact on small and micro businesses

Into what sector and/or subsector the affected businesses fall

- 7.1. In the UK telecoms operators are regulated, primarily, by the Communications Act 2003. They are companies who carry content services either over their own network (a Public Electronic Communications Network or PECN) or using another telecoms operator's network (a Public Electronic Communications Service or PECS). The Communications Act also includes Associate Facilities which are facilities which are essential in the provision of an electronic communication network or service, or support the provision of 'other services' provided by means of that network or service. Examples include telephone calls completed through interactive voice response boxes, TV transmission with MPEG compression supported by compression systems and email supported by e-mail servers.
- 7.2. Examples of PECN and PECS include¹²⁰:
- 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. Public communications providers 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 Public communications providers category.
- 7.4. Ofcom does hold some information on the number of Public communications providers where they:

¹²⁰ Practical Law; Telecoms Quick Guide, [https://uk.practicallaw.thomsonreuters.com/9-503-2464?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&bhcp=1](https://uk.practicallaw.thomsonreuters.com/9-503-2464?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1)

- 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 land, either with the agreement of the landowner or by applying to the County Court¹²¹
 - Have paid administrative fees to Ofcom because they have relevant turnover (turnover made from carrying on any Relevant Activity¹²² 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.¹²³
- 7.6. These two categories are likely to overlap as operators that pay Administrative fees may also have applied for Code powers.
- 7.7. 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).
- 7.8. Table 14 below sets out the number of businesses providing wired and wireless telecommunications services by turnover band¹²⁴. These businesses are likely to include Public communications providers indicating 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 14 - Number of businesses in the Telecommunications division by turnover

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 telecommunications	125	10	10	5	5

¹²¹ 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](#).

¹²² 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.

¹²³ 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

¹²⁴ 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.

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

Impact on businesses (do these impacts fall disproportionately on small and micro business?)

7.9. 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.”¹²⁵

7.10. 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.

7.11. There are three impacts that could fall on small and micro businesses:

- familiarisation costs
- the requirement to provide information to the Secretary of State; and
- the requirement to comply with a Direction issued by the Secretary of State to remove High Risk Vendor equipment from a network.

Familiarisation costs

7.12. The NCSC has published non-binding technical advice to operators in respect of their use of equipment from high risk vendors. This advice is in addition to NCSC’s historic management of high risk vendor use on an advisory basis by NCSC, through advice provided to operators. Furthermore, NCSC has encouraged operators who are considering introducing new vendors into their networks to discuss this with them.

7.13. This guidance is relatively brief and has been publicised widely since its publication. The issue of use of high risk vendors has also been widely discussed by industry prior to this publication and we expect the vast majority of operators to be familiar with the principles of the guidance without significant familiarisation costs.

7.14. As a result we do not consider that familiarisation costs are a significant feature of the costs businesses will incur. We set out in section [Familiarisation costs](#) above an estimate that for each Direction an operator could incur familiarisation costs of £1,000 and that further costs of £300 - £600 would be incurred by each public communications provider. We also note that Directions are more likely to be

¹²⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827960/RPC_Small_and_Micro_Business_Assessment_SaMBA_August_2019.pdf

issued to larger network operators who carry the majority of mobile and fixed network traffic in the UK.

The requirement to provide information

- 7.15. The Secretary of State will need to be provided with accurate information from UK telecoms operators on their vendor arrangements to make decisions on:
- the designation of high risk vendors, and
 - operator compliance with controls set out in directions.
- 7.16. The information required will likely include:
- information on the current use of potential high risk vendors in the operators network;
 - information on the use of designated high risk vendors in the operators' network;
 - information on the use of new vendors, not previously used in the UK network, that may be considered for a new procurement contract, and that will need to be assessed in order to determine whether they may be high risk; and
 - wider information on network details to facilitate the application and assessment of compliance with controls to set out in directions.
- 7.17. The Secretary of State may contact any Public communications providers to request such information. The Secretary of State will determine within what timeframe such information should be submitted, and the frequency with which such information should continue to be submitted where requested.
- 7.18. We do not consider that this information requirement would place a disproportionate requirement on small and medium sized businesses. The costs of gathering information are likely to be related to network size and therefore are not fixed.

The costs of complying with a Direction

- 7.19. The National security powers relating to high risk vendors relate to the procurement of certain types of network equipment and the proportion of network equipment that can be procured from high risk vendors. The costs of implementing the requirements are:
- The need to 'rip and replace' equipment from 4G mobile networks
 - Higher equipment prices for future build
 - The write off and replacement of Huawei equipment already deployed
- 7.20. These costs would not be expected to fall disproportionately on small and micro business because:
- Rip and replace costs are specific to operators with existing 4G networks who are planning on upgrading these networks to a non standalone 5G network.

- Higher equipment costs are proportionate to network size and we do not anticipate that these impacts would fall disproportionately on small and micro businesses.
- In addition, evidence from the Review indicates that Huawei is focused on supplying end to end turn key solutions and that this would not work well for a small operator who would be more likely to build a network incrementally. This indicates that smaller operators are less likely to have Huawei equipment in their networks.
- Write off and replacement of HRV equipment would be proportionate to network size.

Could SMBs be exempted while achieving the policy objectives?

- 7.21. We do not consider an exemption would be appropriate for the national security powers in relations to high risk vendors. An SME may play an important role in a UK telecoms network that is inversely proportional to its size. The policy aim is to ensure powers are available to the Secretary of State to protect the entire UK telecoms network from the national security risk of high risk vendors and a clear gap would remain if SMEs were in some way exempt from such powers.
- 7.22. We also note that small and micro businesses are not exempted from the broader security requirements that are in place through sections 105A - 105D the Communications Act which applies to all PECS and PECN.¹²⁶ Although Ofcom do set out guidance for 'smaller companies' on the measures that would be appropriate for them. Box 6 sets out Ofcom's guidance for 'smaller companies' in relation to security requirements in sections 105A to D of the Communications Act 2003.

¹²⁶ Section 105A to D of the Communications Act 2003 refers to network providers (providers of a public electronic communications network (PECN)) and service providers (providers of a public electronic communications service (PECS)). The Communications Act includes a wider definition of public communications providers the scope of which includes PECN, PECS and also associated facilities which are facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service.

Box 6 - Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003

Small and micro PECNs and PECSs and are currently subject to a security duty under the Communications Act 2003 which includes obligations on Government, Ofcom and industry in relation to the security and integrity of public electronic networks and services, principally in sections 105A to 105D. And that these obligations are derived from the European Union's common regulatory framework for electronic communications networks and services (the Framework).

To assist PECNs and PECSs Ofcom has 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 CPs, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns."¹²⁷

The Act contains requirements under three headings:

- Protecting security
- Breach notification
- Auditing and enforcement

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**¹²⁸. 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."¹²⁹

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

- 7.23. The NCSC high risk vendor guidance is designed to address a specific threat - the risks specific to nation state threat actors or high risk vendors.
- 7.24. The Government is now laying legislation before Parliament seeking additional powers to enforce compliance in this field through the national security powers relating to high risk vendors.¹³⁰
- 7.25. The objectives of the proposed powers are to ensure that the Secretary of State has the ability to manage the risk posed by high risk vendors from a national security perspective. The powers will enable the Secretary of State to impose limits and controls on telecom operator use of HRV products and services.
- 7.26. The Secretary of State will set out controls by issuing directions to operators. Directions should be issued to either individual operators, or to groups of

¹²⁷ Paragraph 1.5.

¹²⁸ Emphasis added

¹²⁹ Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003 2017 Version, paragraph 1.10.

¹³⁰ <https://www.gov.uk/government/speeches/jeremy-wrights-oral-statement-on-the-telecoms-supply-chain-review>

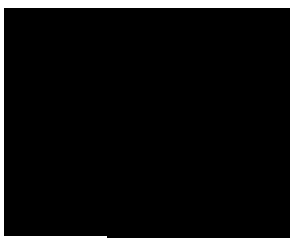
operators, falling within scope of the proposed powers (i.e. that being any public communications provider.

- 7.27. In considering what controls to put in place, the Secretary of State will be informed by NCSC advice.
- 7.28. As we do not present any evidence of a disproportionate impact on small and micro businesses and the requirement for compliance could apply to a company of any size, we do not propose a mitigation for SMBs.

8. Competition impacts

- 8.1. The national security powers in relation to high risk vendors will apply to public communications providers as defined in the Communications Act. It will not directly apply to equipment vendors or managed service providers, though these entities will be impacted.
- 8.2. In our cost benefit analysis we have considered the impacts on communications networks. In this section we consider the impact on competition between vendors and the broader impact on the price of equipment supplied.
- 8.3. This analysis is set out below.

What are the product and geographic markets?



- 8.10. For the purposes of this impact assessment we therefore consider the impact of the measures on the markets they are proposed in. These are:
 - the 5G mobile core equipment and full fibre fixed core.¹³¹
 - the 5G mobile access equipment and full fibre fixed access equipment.
- 8.11. We also consider the market for 4G/3G/2G access equipment to the extent that this is linked to the market for 5G mobile access equipment.



- 8.14. For the purposes of this impact assessment the focus is on the UK supply-chain taking into account the broader geographic context where relevant.

Establishing the baseline

- 8.15. The supply chain for telecoms equipment is complex involving many different market segments and many more suppliers. Many of these suppliers are global companies for whom the UK is a relatively small market. Our focus is on equipment vendors supplying active equipment into the product markets identified in section [What are the product and geographic markets?](#).
- 8.16. The global telecoms equipment market for network operators is dominated by three global players – Huawei, Ericsson and Nokia. Other players include Samsung, CISCO, Juniper, Ciena and ZTE – however, their participation varies across different parts of the network.

¹³¹ We also expect an impact on the transmission and transportation market as a result of NCSC advice that NCSC's Huawei mitigation strategy would exclude Post-sanction data transport equipment. However, we do not estimate an impact in this market as we assume operators can find alternative suppliers for this equipment without additional cost.

- 8.17. In the UK, there is a high concentration in certain market segments and the leading players are also Huawei, Ericsson and Nokia. [REDACTED]
- 8.18. Huawei is the leader in the 4G mobile access market in the UK. It has the highest market share in this segment at c.35% overall.¹³² It is also the leader in fixed access in the UK. Its market share in full fibre (FTTP) is c.45%, whilst its reported market shares in other fixed network segments are lower.
- 8.19. Huawei faces competition mainly from Nokia and Ericsson in the UK mobile and fixed access equipment markets, although the latter does not have a strong position in the fixed access market. Ericsson is also active in the mobile core market while Nokia is also active in both the mobile and fixed core markets. Samsung has a limited presence in the provision of mobile and fixed network equipment in the UK.¹³³
- [REDACTED]

Will the measure directly limit the number or range of suppliers?

- 8.23. Option 1 and Option 2 would both be expected to directly limit the number of suppliers. They will do this by:
- Preventing any company identified as a high risk vendor from supplying the 5G mobile equipment core and full fibre fixed core markets - 'the Core Exclusion'.
 - Restricting the use of high risk vendor equipment in 5G mobile access and full fibre fixed access markets - 'the Access Restriction'.
 - Preventing any company identified as a high risk vendor from supplying the 5G mobile access and full fibre fixed access markets - 'the Access Exclusion'.
- 8.24. The difference between Option 1 (the Access Restriction) and Option 2 (the Access Exclusion), in relation to our assessment of the competition impact, is related to timing.¹³⁴ Under the Restriction, telecoms operators must stop purchasing any new 5G equipment after 31 December 2020. They must also remove all Huawei equipment from 5G networks by the end of 2027. Full fibre operators should transition away from purchasing new Huawei equipment, and a technical consultation¹³⁵ would determine the precise timetable from which point fixed operators should stop procuring affected Huawei equipment.
- 8.25. Under Option 2 (the Access Exclusion) we assume that both 5G and full fibre operators stop purchasing Huawei equipment from 2020 and remove existing Huawei equipment by 2023.
- 8.26. A company can be identified as a high risk vendor by reference to a list of non-exhaustive criteria set out by NCSC. These criteria relate to the vendor's

¹³² DCMS estimate based on total number of mobile sites, 2018.

¹³³ Samsung is active in 5G in other countries such as South Korea and the US. However their lack of 2G together with UK operators' desire to use non-standalone 5G deployments limits Samsung's potential as a 5G supplier in the short-term.

¹³⁴ The full difference between Option 1 and Option 2 is set out in section What options have been considered?


¹³⁵ The consultation is being planned for the autumn.

strategic position and scale, the quality and transparency of the vendor's engineering practices and cyber security controls, the past behaviour and practices of the vendor, the vendor's resilience and a number of considerations relating to the ownership and operating location of the vendor.

What is the impact of limiting the number of suppliers?

- 8.27. The national security powers relating to high risk vendors will restrict the number and type of suppliers according to suppliers characteristics. This restriction is akin to a form of licensing, a tool that is commonly used to make sure that suppliers have a minimum level of competency or are fit to operate in a market. For example, in the legal and accountancy professions only persons holding certain qualifications are allowed to work in that profession.
- 8.28. This restriction will work in the same way as a licensing scheme where vendors require an implicit licence¹³⁶ to operate unrestricted in these markets; and this licence is only available to non-high risk vendors. Equally high risk vendors require an approved mitigation strategy to operate in these markets under the restrictions set out.
- 8.29. Whilst licensing has clear benefits in terms of the license objectives - in this case the security and resilience of UK telecoms networks - it can also harm competition by restricting the number of suppliers. The following are potential impacts identified in the Competition Impact Assessment guidelines¹³⁷:
- reduced numbers of suppliers which may help to keep price levels high or lead to an increase in prices
 - restrict choices and ultimately result in reduced supply
- 8.30. We now consider whether the proposed measures - national security powers relating to high risk vendors - will result in these impacts and how that might affect competition. In particular we consider the impact of:
- Limiting or prohibiting the use of products and services from high risk vendors in the Access markets
 - Prohibiting the use of products and services from high risk vendors in specific network functions

Will reduced numbers of suppliers affect prices?

- 8.31. In our modelling for this impact assessment we assume that the reduction in the number of suppliers as a result of the Restriction or Exclusion (Option 1 and 2) affect prices in the Access market (leading to an increase in prices of 12.5% in the Mobile Access market and 12.5% in the Fixed Access market). In the Core markets we assume that, despite the Exclusion, prices remain unchanged.
- 

¹³⁶ Vendors will not be required to obtain a licence to operate; the restrictions operate by designating certain vendors as high risk vendors.

¹³⁷

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/460787/Competition_impact_assessment_Part_2_-_guidelines.pdf, Paragraph 3.21.

- [REDACTED]
- 8.34. As set out in the section [Establishing the baseline](#) above the markets that we are considering are all relatively concentrated [REDACTED]
- 8.35. As well as being relatively concentrated there may be some level of differentiation between providers in these markets reducing the competitive pressure that competing providers provide. [REDACTED]
- [REDACTED]

The Access Restriction and Exclusion would both affect the level of buyer power

- 8.39. The Access Restriction and Exclusion would have a clear effect on concentration in Access markets directly reducing the number of suppliers.
- 8.40. This reduction in the number of suppliers is likely to affect the level of bargaining power that operators currently hold. [REDACTED]
- 8.41. In Fixed Access whilst there are more suppliers in total, the lack of alternative scale vendors is likely to mean that buyer power is significantly affected.
- 8.42. The ability to dual source and switch operators are key factors determining the level of buyer power that operators have in access equipment markets.
- 8.43. However, operators will continue to benefit from other sources of buyer power including; their global networks and procurement strategies, size of contracts and the UK's strategic importance/growth potential in fibre networks.

What is the impact on prices in Access networks

- 8.44. In this impact assessment we assume that the Restriction and the Exclusion would lead to prices for Access equipment increasing in the short term. This would happen as:
- operators will face higher equipment prices if use of Huawei is restricted; and
 - supply side competition is reduced leading to generally higher prices.
- 8.45. We assume the price rises that result from a reduction in supply side competition affect all the operators, even those that are not planning to use Huawei equipment as the impact on competitive tension will be felt across all vendors.
- 8.46. We estimate that under Option 1 and Option 2 prices increase by 12.5% in 5G access networks and 12.5%¹³⁸ in full fibre access networks and that these price effects will persist until network roll outs are completed.¹³⁹

Other factors will affect Access market prices

[REDACTED]

¹³⁹ In our modelling we have assumed all costs are incurred in the implementation period. This reflects both a conservative approach of bringing costs forward and the fact that operators might agree prices and purchase equipment in advance of installing it.

- 8.47. Huawei has benefited from a large domestic market supported by state subsidies, and its growth in the UK has been accelerated by offering what are perceived to be higher quality, lower priced equipment to operators.
- 8.48. This is likely to mean that both the Access Restriction and Exclusion would lead to inflationary pressures as operators replace Huawei equipment with more expensive equipment from other suppliers.¹⁴⁰
- 8.49. On the other hand, new vendors may enter the market to take advantage of the space created by the restrictions on high risk vendor equipment in Access networks. This could take place both in the short term - where a global scale vendor enters the UK market - or in the longer term - where smaller vendors grow to compete in the access network over time.

The Core Exclusion will reduce the number of suppliers in the Core markets

- 8.50. In the Core markets the effect of the Exclusion will be to reduce the number of vendors in markets in which Huawei is present. Depending on how concentration is measured and whether the HRV market share is reallocated to other incumbents, this will be likely to increase the level of market concentration.
- 8.51. However, in the markets for Core equipment there is also greater scope for operators to use different vendors for different elements of the networks. In addition, the refresh rate for these markets is faster giving operators more opportunity to switch between vendors. This is particularly important as new (specialised) vendors are entering these markets.

The Mobile Core

- 8.52. Huawei has a small and declining share of the UK mobile core market with its market share across the core and transport sectors estimated to be 15%.¹⁴¹ Operators, including Vodafone¹⁴² and EE¹⁴³ have a publicly-stated position of not using Huawei in the mobile core.
- 8.53. Globally, HRVs have a more significant market share in the core markets - estimates by Dell'Oro put Huawei's market share in the mobile core at 25% and ZTE's share at 10%.¹⁴⁴ Historically, the involvement of HRVs in UK telecoms networks has been managed on an advisory basis by NCSC, through advice provided to operators. This advice may be the cause of the limited presence of HRVs in the UK core markets. Equally it may reflect UK operators' decisions on vendor selection in the context of the UK market.

¹⁴⁰ In our modelling of the impact of the Restriction in Access markets (set out in [Box 5](#) - we include the effect of inflationary pressures through applying higher equipment costs for operators that replace Huawei equipment with equipment from another vendor).

¹⁴¹ <https://www.endersanalysis.com/reports/huawei-and-5g-identifying-risks>

¹⁴² <https://www.theguardian.com/business/2020/feb/05/vodafone-to-remove-huawei-from-core-european-networks>

¹⁴³ <https://www.reuters.com/article/us-bt-5g/ee-keeps-huawei-in-first-british-5g-network-but-halts-handsets-idUSKCN1SS0SQ>

¹⁴⁴ <https://www.fiercewireless.com/tech/ericsson-holds-slight-lead-over-huawei-mobile-core-market>

8.54. Based on the global counterfactual the impact of the Exclusion in the mobile core is a reduction in the number of main vendors from five to three¹⁴⁵ with the remaining players increasing their market share by 35% collectively. Based on the UK mobile core market counterfactual, the impact of the Exclusion is a reduction in the number of vendors from four to three with the remaining players increasing their market share by 15%.

The Fixed Core

8.56. [REDACTED] Overall, the supply of fixed core equipment is characterised by a large number of smaller, alternative vendors. [REDACTED]

[REDACTED]

8.60. Based on this evidence we do not expect the Exclusion would lead to a price impact in Core markets. This is due to the number of vendors active in the core, operator buyer power and the presence of global core vendors not active in the UK.

Will the measures restrict choices for operators?

- 8.61. Huawei is a leading player in the supply of mobile and fixed access equipment in the UK and globally. Its two main competitors are Nokia and Ericsson. In contrast Huawei has a small and declining share of the mobile core market with operators publicly-stated position of not using Huawei in the mobile core. While Huawei has a small presence in fixed core networks, it is used by a small number of operators.
- 8.62. This indicates that the national security power will restrict choices for operators by excluding it from operating in Core markets and restricting its presence in Access markets.
- 8.63. However, the NCSC found in their assessment of Huawei - which they set out in their HRV guidance - that:
'our experience has shown that Huawei's cybersecurity and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the

¹⁴⁵ In practice there are more than five vendors in core - these are the top ones but by no means the only (viable) ones.

remediation of technical issues reported in the 2018 report and highlighted “further significant technical issues” that had not previously been identified;¹⁴⁷

- 8.64. This indicates that whilst Huawei equipment is currently being chosen by operators - they may not prioritise security in vendor selection which is consistent with the findings of the Review.

Impact on innovation

- 8.65. Finally, the measures could lead to a worsening of non-price attributes of the products being offered - for example, innovation. Huawei has been considered a disruptor in the market and is perceived to have driven down prices. The measures could reduce the impact of this type of innovation on the UK market
- 8.66. However, the UK is a small player in global markets and innovation is likely to be driven by global trends. Therefore the measures are unlikely to impact on total investment in R&D by global scale vendors. In addition, given the UK’s position as a strategically important market for vendors it is also likely that new technologies will continue to reach the UK where vendors may seek to demonstrate track record to other markets internationally.

Quantified impacts Access Networks

- 8.67. For the purposes of this impact assessment we have modelled the impact of a price increase in the Access markets as a result of Option 1 and Option 2. We estimate that the impact of the Option 1 and Option 2 will lead to price increases of 12.5% in both Access markets.¹⁴⁸
- The impact of these price increases is estimated using the Supply Chain Review model which is described in Box 5 above. In addition to these increases in the general price level the model also assumes that operators pay higher prices for alternative equipment when they switch away from Huawei. So for operators already using Huawei equipment our predicted cost impact would be 25% in total.
- 8.68. These impacts are included in our estimates in the section Direct costs and benefits to business calculations alongside the equipment costs which are set out in section What are the costs of the policy options in the Access network?
- 8.69. We can compare these price impacts with data from the OECD Competition Impact Assessment Tool. This database has used more than 300 research studies of the impact of procompetitive regulatory reform, the vast majority of which are taken from developed countries that are members of the OECD.
- 8.70. We can use this data as a ‘rule of thumb’ to estimate the price effect of introducing a regulatory restriction that impacts on competition. On this basis a regulatory proposal that limits the ability of some types of suppliers to provide a good or

147

service, based on the average price effect from before-and-after empirical studies, could lead to a 15% price rise.¹⁴⁹

- 8.71. As the HRV restrictions impact a limited number of suppliers we consider that this is consistent with our estimates of price increases below 15% in the Access markets.

Quantified Impacts Core

- 8.72. In the Core markets we assume that there is no price impact. In the core markets the effect of the Exclusion will be to reduce the number of vendors in markets in which Huawei is present. Again, depending on how concentration is measured and whether the HRV market share is reallocated to other incumbents, this will be likely to increase the level of market concentration.
- 8.73. However, in the markets for core equipment there is greater scope for operators to use different vendors for different elements of the networks. In addition, the refresh rate for these markets is faster giving operators more opportunity to switch between vendors. This is particularly important as new (specialised) vendors are entering these markets.

¹⁴⁹ Table 5, Competition Impact assessment guidelines, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/460787/Competition_impact_assessment_Part_2_-_guidelines.pdf

9. A summary of the potential trade implications of measure

Potential impacts on imports or exports

- 9.1. The national security power could impact the telecoms equipment supply chain by reducing telecoms operators use of products supplied by telecoms equipment vendors that have been designated as high risk vendors. As a result, the Access Restriction and Core Exclusion could affect the import of goods. We do not expect there will be an impact on exports.
- 9.2. NCSC has fed in a non-exhaustive list of criteria which NCSC applies when identifying vendors as high risk vendors to the supply chain review.¹⁵⁰
- 9.3. The two companies that the NCSC consider to be HRVs currently are Huawei and ZTE, both Chinese equipment vendors. The consequent impact on imports from China is detailed in the next section.

Direct or indirect impact on the value of overall trade or investment flows

- 9.4. We have not estimated the impact on the value of overall trade or investment flows quantitatively. Our cost analysis looks at the costs of replacing high risk vendor equipment in the UK telecoms supply chain but not if the replacement equipment would be provided by a domestic or international supplier. However, we note that all of the scale vendors in the telecoms equipment supply chain are global companies which are headquartered outside the UK. For example, Nokia is headquartered in Espoo, Finland; Ericsson is headquartered in Stockholm, Sweden; Cisco is headquartered in San Jose, California and Samsung is based in Suwon, South Korea.
- 9.5. We therefore do not expect a significant impact on total trade or investment flows on the basis that any reduction in imports from a high risk vendor will be offset by an increase in imports from another global vendor.
- 9.6. It is difficult to accurately estimate the direct impacts of the Core Exclusion and Access Restriction on Chinese imports, given uncertainties about how the market would have developed absent intervention.
- 9.7. [REDACTED]. In terms of the impact on imports, it is difficult to estimate the amount of Huawei and ZTE equipment currently imported into the UK. We do have statistics of the total imports of telecoms equipment from China, from a 2018 House of Commons briefing report. The report states that “in 2018, the UK’s single largest import from China was telecoms equipment, valued at £6 billion, representing 15% of all UK goods imports from China”.¹⁵¹ We do not know what proportion of this comes from Huawei and ZTE.
- 9.8. In terms of indirect impact, the national security power is expected to improve the investment flows into the UK as they will improve the security of UK telecoms infrastructure. Malcolm Campbell, European Union (EU) Cyber Resilience for

¹⁵⁰ https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks#section_4

¹⁵¹ House of Commons Briefing Paper Number 7379, 5 November 2019. Statistics on UK trade with China

Development Project Leader, speaking at the 12th Annual National Conference on Cyber Security in 2019, stated that "a mature cyber security apparatus and high resilience in both the State and private sector was a significant consideration for investors when planning Foreign Direct Investment (FDI)".¹⁵²

Different requirements for domestic and foreign businesses?

- 9.9. The national security powers apply to UK telecommunications networks and their supply chains insofar as they may place a restriction on the networks use of equipment supplied by high risk vendors. Where these powers are used they will apply to UK networks vendors based on criteria which include, among other things, the ownership and operating location¹⁵³.
- 9.10. These criteria are driven by security requirements rather than location of a vendor; however, the nature of these requirements indicates that they would apply to a foreign and not domestic vendors.
- 9.11. The criteria are set out by the NCSC in their advice on the use of high risk vendors in UK telecoms networks¹⁵⁴. They are:
 - The influence which the domestic state apparatus can exert on the vendor (both formal and informal);
 - Whether the relevant domestic state and associated actors possess an offensive cyber capability that might be used to target UK interests;
 - Whether a significant component of its business operation is subject to domestic security laws which allow for external direction in a manner that conflicts with UK law.

The Basis of Different treatment

- 9.12. In the NCSC statement published on 28th January 2020, the NCSC states the reasons NCSC continues to consider Huawei an HRV, including:
 - 'Huawei has a significant market share in the UK already, which gives it a strategic significance;
 - it is a Chinese company that could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
 - we assess that the Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and our interests;
 - Our experience has shown that Huawei's cybersecurity and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified; and

¹⁵²<http://www.ft.lk/front-page/Strengthening-cyber-security-can-boost-FDI-say-experts/44-687887>

¹⁵³ [NCSC advice on the use of equipment from high risk vendors in UK telecoms networks](#), 2020.

¹⁵⁴ Ibid

- A large number of Huawei entities are currently included on the US Entity List. Although we do not have knowledge as to whether these entities will remain on the US Entity List, this listing may have a potential impact on the future availability and reliability of Huawei's products.'

10. Monitoring and Evaluation

How is the current system monitored

- 10.1. The NCSC is the UK's technical authority for cyber threats. It is part of the Government Communications Headquarters (GCHQ).
- 10.2. The NCSC acts as the 'computer security incident response team' or CSIRT. This means it monitors incidents, provides early warnings, disseminates information, conducts cyber threat assessments and provides general technical support to competent authorities.
- 10.3. In the telecoms sector one of the NCSC's key objectives is to maintain a deep understanding of the cyber risks and develop strategies to manage those risks. The NCSC's assessment of those risks shapes the way in which each vendor's presence is managed in the telecoms supply chain – albeit today this is on a voluntary, not mandatory basis.
- 10.4. This risk based strategy leads to a variety of approaches aimed at increasing understanding of areas, including engineering and design processes, ongoing product support and vulnerability remediation. The level of assessment of different vendors is proportionate to the level of risk identified.
- 10.5. The UK has a rigorous strategy in place for managing the risks arising from the involvement of Huawei in parts of the UK's critical national telecommunications infrastructure, including through the Huawei Cyber Security Evaluation Centre (HCSEC) and the Oversight Board.
- 10.6. The 2018 and 2019 Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board reports have highlighted major quality and security issues with Huawei's engineering, leading to the Board only being able to provide 'limited assurance' that risks to UK national security from Huawei's involvement in the UK critical networks have been sufficiently mitigated.

What external factors will impact on the success of the national security power

- 10.7. The national security powers in relation to high risk vendors are 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.
- 10.8. 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 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.

- 10.9. 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.'¹⁵⁵

How will the national security powers in relation to high risk vendors be monitored

- 10.10. The objectives of the proposed powers are to ensure that the Secretary of State has the ability to manage the risk posed by high risk vendors from a national security perspective. The powers will enable the Secretary of State to impose limits and controls on a telecoms operator's use of HRV equipment products and services. The Secretary of State will be able to reach a decision in future on operator compliance with any controls imposed. The policy objective will have been met if operators have complied with their obligations and as a result the national security risk has been managed.
- 10.11. Operator compliance with their obligations will be regularly monitored as part of the proposed framework. If operators are not complying with their obligations, the Secretary of State may need to consider strengthening the sanctions regime to improve the effectiveness of the controls imposed.
- 10.12. All data necessary to assess whether the policy has been successful will be collected as part of the ongoing compliance framework. It is not anticipated that any further information will be required.
- 10.13. A Post Implementation Review of the proposed powers will take place at the latest by 01/01/2026.

¹⁵⁵ Ibid, page 24.