**Title:** Electronic Communications (Security Measures) Regulations
**IA No:**

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

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

**Other departments or agencies:**

# Impact Assessment (IA)

**Date: 22/06/2022**

**Stage: Final**

**Source of intervention: UK government**

**Type of measure: Secondary Legislation**

**Contact for enquiries:** Jibirila Leinyuy
jibirila.leinyuy@dcms.gov.uk

Shamraze Mahmood
shamraze.mahmood@dcms.gov.uk

## Summary: Intervention and Options

**RPC Opinion:** GREEN - 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 |
|---|---|---|---|
| £ -4103.9m | -4102.9m | £ 470.5m | Qualifying provision |

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

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

In 2018-2019, Department for Digital, Culture, Media and Sport (DCMS,) supported by the National Cyber Security Centre (NCSC), undertook a comprehensive review of the supply arrangements for telecoms critical national infrastructure. The conclusions and recommendations of this UK Telecoms Supply Chain Review were set out in a report, published in July 2019[1]. The Review's starting-point was a set of concerns about the provision of equipment for both 5G and full fibre networks. These concerns were largely related to the overall quality of software engineering, under-investment in cyber security, and a growing dependence on a small number of viable vendors, including high risk vendors.

Telecommunications providers are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks. However, there can be tensions between commercial priorities and

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

security concerns, particularly when these impact on costs and investment decisions. The flaws identified in the Review's report were the result of practices that may have achieved good commercial outcomes but resulted in poor cyber security.

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

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

The government aims to improve cyber security standards and practices across the telecoms sector through a new, robust security framework set out in the Telecommunications (Security) Act 2021 ('the Act')[2]. The government published accessible information on the objectives of the Act in its factsheets, available online[3].

The security framework applies to providers of public electronic communications networks and services[4], and consists of three layers:

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

The Electronic Communications (Security Measures) Regulations, which form the second layer of this new framework, are vital to its success. The regulations have been developed from detailed security analysis conducted by the NCSC that used a threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[5]. An early draft of the regulations was published in January 2021 to gather industry feedback[6]. The draft regulations were published for formal consultation, alongside a consultation stage assessment, in March 2022 and have since been updated to account for that feedback. They propose to address the security risks facing public networks and services by providing appropriate and proportionate security requirements in law with which public telecoms providers must comply. Ofcom, as the independent telecoms regulator, will be responsible for monitoring and enforcing compliance with the statutory requirements.

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

[2] Telecommunications (Security) Act 2021

[3] Telecommunications (Security) Bill: Factsheets 2020

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

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

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

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

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

- **Option 0 (Do nothing):** This option involves DCMS taking no action to address the security issues identified in section 1 and retaining the pre-existing obligations in sections 105A to 105D of the Communications Act prior to the Telecommunications (Security) Act coming into force. This is the counterfactual option against which the incremental impact of all other options are considered.
- **Option 1 (Preferred option) -** The Act places high level security duties on providers and specific security regulation requirements are set out in secondary legislation draft regulations. These regulations requirements are applied appropriately to providers of public telecommunications networks and services (PECN and PECS) in a way that is appropriate and proportionate in different ways, reflecting the characteristics of network security compared to service security. A code of practice is published as best practice guidance for industry to follow and for Ofcom to take into account in ensuring compliance with the legal obligations. Implementation is phased by date, depending on the relative complexity of the measures, and by type of provider. Analysis in this document therefore assesses expected costs and benefits against the implementation timeframes below:
  - **31 March 2024 (the largest ('Tier 1') providers only)** - completion of the lowest complexity and least resource-intensive actions
  - **31 March 2025** - completion of the remaining low complexity actions achievable with minimal resource allocations by for Tier 1; and both the lowest complexity and least resource-intensive for actions by for smaller (' Tier 2') providers
  - **31 March 2027** - completion of actions which require devotion of new resources and a degree of complexity (Tier 1 and Tier 2)
  - **31 March 2028** - completion of high complexity and resource-intensive actions that must take account of wider change programmes or require deeper, strategic solutions (Tier 1 and Tier 2).
- **Option 2 - (Implementation Plus):** The specific security requirements are set out in the draft regulations as in the preferred option but implementation is phased by date only (not by *type* of provider).; This options guidance sets out a single set of implementation dates applying to all Tier 1 and Tier 2 providers . The 'implementation plus' option differs from option 1 as it sets out a tighter timescale for Tier 1 and also for more specifically Tier 2 providers. The proposed implementation dates for both Tier 1 and Tier 2 providers are:
  - **31 March 2023** - proposed completion of the most straightforward actions achievable with minimal resource allocations
  - **31 March 2025** - proposed completion of actions which require devotion of new resources and a degree of complexity
  - **31 March 2026** - proposed completion of actions that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions.

| | | | | |
|---|---|---|---|---|
| Is this measure likely to impact on international trade and investment? | | Yes | | |
| Does implementation go beyond minimum EU requirements? | | N/A | | |
| Are any of these organisations in scope? | **Micro** No | **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?** It will be reviewed. **If applicable, set review date:** October 2027

***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 : *Alison Kilburn* Date: 22/06/2022

# Summary: Analysis & Evidence

Policy Option 1

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

**FULL ECONOMIC ASSESSMENT**

| Price Base Year | PV Base Year | Time Period Years | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| 2022 | 2022 | 10 | **Low: - -5800.5** | **High: -2233.7** | **Best Estimate: -4103.9** |

| COSTS (£m) | Total Transition (Constant Price) Years | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|
| **Low** | 1142.1 | 142.8 | **2233.7** |
| **High** | 3274.2 | 332.4 | **5800.5** |
| **Best Estimate** | 2217.4 | 245.7 | **4103.9** |

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

The impact assessment conducted for the Telecommunications (Security) Bill was unable to estimate costs to providers. This was due to a number of issues, including the need for providers to prioritise resources to mitigate the impacts of the COVID-19 pandemic meaning they were not able to return a structured survey on the impacts of the Bill.

We subsequently assessed the impacts of both primary and secondary legislation through a survey to estimate the costs that businesses would incur in implementing the early illustrative draft version of the Electronic Communications (Security Measures) Regulations published in January 2021. Following the decision of the Minister to consult with industry on the subsequent draft regulations and code of practice, we issued another cost survey on 1 March 2022 to better understand the impacts of the Electronic Communications (Security Measures) regulations which will be published in early September 2022.

The results of this survey highlighted the significant costs of implementing the regulations and estimated these costs for the largest providers (those expected to fall into Tiers 1 and 2[7]). In summary, we found that over the impact assessment period 2022-2031, in total, Tier 1 and 2 providers:

- could incur present value one-off costs in a range from £1,000m to £2,600m in present value terms. These costs are likely to be spread over a number of years.
- could incur present value annual ongoing costs in a range from £100m to £240m per year in present value terms.

We have assumed that the one-off costs are incurred early, over the years 2022-2027, to comply with the implementation timeframes stated under this preferred option. This conservative approach assumes that the largest providers (Tier 1[8]) will implement the requirements straight away with the smaller providers (Tier 2[9] and

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

[8] Tier 1 - public telecoms providers with relevant turnover in the relevant period of £1bn or more

[9] Tier 2 - public telecoms providers with relevant turnover in the relevant period of more than or equal to £50m but less than £1bn

Tier 3[10]) commencing implementation a year after. This approach aligns with the feedback we received via the public consultation, cost survey and clarification interviews with smaller providers who did not state they would comply with the regulations as early as possible.

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

We have also estimated the costs to Tier 3 providers. We used cost survey data and qualitative feedback to estimate that in total, Tier 3 providers could incur present value one-off costs in a range from £210m to £1,060m (a central estimate of £630m) and present value annual ongoing costs in a range from £27m to £77m per year. It is important to note that there is no expectation for Tier 3 providers to follow the code of practice but they will be expected to comply with the regulations to a level which is appropriate and proportionate. In addition, Ofcom has stated that Tier 3 providers will not be part of the Tier 1 and Tier 2 compliance monitoring set out in their Draft general statement of policy under section 105Y of the Communication Act 2003[11]. However, Tier 3 providers will still be required to comply with their legal obligations, and Ofcom could use its powers to investigate potential breaches and take enforcement action where necessary. This supports our view that Tier 3 providers are unlikely to be disproportionately affected by the regulations and code of practice. Similar to last year, we again received a limited response to the latest survey from Tier 3 providers. As a result of the limited survey response from Tier 3 providers, we have relatively low confidence that these estimates are an accurate representation of the true costs incurred by such providers.

The survey also gathered data on familiarisation costs for all providers in scope of the regulations. We found that there will likely be significant familiarisation costs as providers get ready to embed the regulations into their business processes. However, these remain small in proportion to the total costs to business and total £4.6m - £7.8m for providers across all Tiers.

In addition to costs of implementing the regulations, we expect Tier 1 and 2 providers to incur costs in reporting compliance with the regulations and these costs will depend on the frequency and style of compliance reporting required. We have estimated these costs based on metrics for cost of compliance which we use as a proxy. These indicate a present value cost to Tier 1 and 2 providers of approximately £6m annually. We have assumed that Tier 2 reporting costs will commence one year after Tier 1's due to the implementation timeline concessions afforded to smaller providers under our preferred option 1. However, these costs could change depending on Ofcom's final reporting framework.

Finally, Ofcom expects to incur costs associated with monitoring and enforcing industry compliance of £53m - £70m over the impact assessment period. As a result of the Telecommunications (Security) Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, having regard to the code of practice in their regulatory work. The Department for Digital, Culture, Media & Sport (DCMS) will also incur additional costs in providing administrative support for the Secretary of State under the new security regime. These are expected to total £0.9m - £1.4m over the impact assessment period.

[10] Tier 3 - public telecoms providers whose relevant turnover in the relevant period is less than £50m

[11] Annex 5: Draft general statement of policy under section 105Y of the Communications Act 2003 - https://www.ofcom.org.uk/__data/assets/pdf_file/0027/233568/annex-5-draft-s105A-Z-procedural-guidance.pdf

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

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

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

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

Estimates suggest that the cost of a security breach or cyber attack for a UK telecoms company could be anywhere in the range of £4,000 to £250m. We estimate that the total central cost over the impact assessment period of security compromises for PECN and PECS providers is £3,300m, within a range of £2,000m - £3,900m. Within this estimate, we have assumed that, over the next ten years, there will be two severe incidents (in line with historic precedent) which reduce the share price of the affected provider, resulting in a loss of £120m per incident. The new security framework will reduce the cost impact of security compromises, reducing the total cost of such compromises. However, we have not estimated the proportion of costs that would be avoided and have therefore not included these benefits in the NPV and EANDCB.

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

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

| **Key assumptions/sensitivities/risks** | **Discount rate (%)** |
|---|---|
| At the time of writing this impact assessment, inflation has increased to 9.0% (CPI) in the UK. This is a result of inflation rising by 7.5% over the 12 month period from April 2021. We think that high levels of inflation will likely inflate our final cost and benefits estimates equally. It would be expected that a rise in cost estimates would be driven by increased input costs for telecoms providers e.g. wage and resource costs when complying with the regulations. Furthermore, we think our benefits estimates would be inflated by the costs of avoided security compromises also increasing. As a result, we do | 3.5 |

not believe inflation will broadly affect our analysis and have used the standard Green Book discount rate of 3.5% for our appraisal.

Due to a lack of available data we were unable to recommend sound upper and lower bound optimism bias levels for our benefits estimates (avoided security compromises and 5G use cases). As an alternative we have used sensitivity analysis to check the plausible range for our estimated benefits per paragraph 4.1 in HMT's Green Book supplementary guidance[12] on optimism bias.

We have undertaken a 10 year appraisal period as this is a legislative policy, which aligns with Green Book guidance

It is also the case that:

- We do not know how providers will practically implement the guidance in the code of practice once it is in place or to what degree existing or planned security processes will be in line with the code.

We have used estimates of costs from providers to estimate the total cost to business of the regulations published in September 2022 . There is a risk that the ultimate cost to business once the legislation is implemented may vary from businesses' best estimate at this stage.

It is also the case that:

- We do not know how providers will practically implement the guidance in the code of practice once it is in place or to what degree existing or planned security processes will be in line with the code.
- 
- The code of practice will be reviewed regularly and will be updated as new threats emerge and technologies evolve. Any such review and consultation on changes could affect the costs to business.

**BUSINESS ASSESSMENT (Option 1)**

| **Direct impact on business (Equivalent Annual) £m:** | | | **Score for Business Impact Target (qualifying provisions only) £m:** |
|---|---|---|---|
| **Costs: 470.5** | **Benefits: 0** | **Net: 470.5** | 2352.4 |

[12] Green Book supplementary guidance on optimism bias - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191507/Optimism_bias.pdf

# Summary: Analysis & Evidence

Policy Option 2

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

**FULL ECONOMIC ASSESSMENT**

| Price Base Year 2022 | PV Base Year 2022 | Time Period Years 10 | Net Benefit (Present Value (PV)) (£m) | | |
|---|---|---|---|---|---|
| | | | **Low: -5946.9** | **High: -2417.4** | **Best Estimate: -4209.2** |

| COSTS (£m) | Total Transition (Constant Price) Years | | Average Annual (excl. Transition) (Constant Price) | Total Cost (Present Value) |
|---|---|---|---|---|
| **Low** | 1141.9 | | 158.4 | 2417.4 . |
| **High** | 3274.1 | | 339.4 | 5946.9 |
| **Best Estimate** | 2217.4 | | 250.8 | 4209.2 |

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

The impact assessment conducted for the Telecommunications (Security) Bill was unable to estimate costs to providers. This was due to a number of issues, including the need for providers to prioritise resources to mitigate the impacts of the COVID-19 pandemic meaning they were not able to return a structured survey on the impacts of the Bill.

We subsequently assessed the impacts of both primary and secondary legislation through a survey to estimate the costs that businesses would incur implementing the early illustrative draft version of the Electronic Communications (Security Measures) Regulations published in January 2021. Following the decision of the department to consult with industry on the subsequent draft regulations and code of practice, we issued another cost survey on the 1st March 2022 to better understand the impacts of the Electronic Communications (Security Measures) regulations which will be published in early September 2022. The results of this survey highlighted the significant costs of implementing the regulations and estimated these costs for the largest providers (those expected to fall into Tiers 1 and 2). In summary we found that over the impact assessment period 2022-2031. In total, Tier 1 and 2 providers:

- could incur present value one-off costs in a range from £1,040m to £2,500m in present value terms. These costs are likely to be spread over a number of years.
- could incur present value annual ongoing costs in a range from £120m to £250m per year in present value terms.

We have assumed that the one-off costs are incurred earlier when compared to the preferred option 1, over the years 2022-2025 to comply with the implementation timeframes stated under option 2 ('implementation plus'). This approach assumes that the largest providers and medium sized providers (Tier 1 and Tier 2) will implement the measures in the code of practice straight away. We have assumed that Tier 3 providers will again begin implementation a year after (as per option 1). This approach aligns with the feedback we received via the public consultation and cost survey with smaller providers who did not state they would comply with the regulations as early as possible.

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

We have also estimated the costs to Tier 3 providers. We used cost survey data and qualitative feedback to estimate that in total, Tier 3 providers could incur present value one-off costs in a range from £210m to £1,060m (a central estimate of £630m) and present value annual ongoing costs in a range from £27m to £77m per year. It is important to note that there is no expectation for Tier 3 providers to follow the code of practice but they will be expected to comply with the regulations to a level which is appropriate and proportionate. In addition, Ofcom has stated that Tier 3 providers will not be part of the Tier 1 and Tier 2 compliance monitoring set out in their Draft general statement of policy under section 105Y of the Communication Act 2003[13]. However, Tier 3 providers will still be required to comply with their legal obligations, and Ofcom could use its powers to investigate potential breaches and take enforcement action where necessary. This supports our view that Tier 3 providers are unlikely to be disproportionately affected by the regulations and code of practice. Similar to last year, we again received a limited response to the latest survey from Tier 3 providers. As a result of the limited survey response from Tier 3 providers, we have relatively low confidence that these estimates are an accurate representation of the true costs incurred by such providers.

The survey also gathered data on familiarisation costs for all providers in scope of the regulations. We found that there will likely be significant familiarisation costs as providers get ready to embed the regulations into their business processes. However, these remain small in proportion to the total costs to business and total £4.6m - £7.8m for providers across all Tiers.

In addition to costs of implementing the regulations, we expect Tier 1 and 2 providers to incur costs in reporting compliance with the regulations and these costs will depend on the frequency and style of compliance reporting required. We have estimated these costs based on metrics for cost of compliance which we use as a proxy. These indicate a present value cost to Tier 1 and 2 providers of approximately £6.7m annually. We have assumed that Tier 1 and Tier 2 reporting costs will commence at the same time as implementation concessions are not afforded to Tier 2 providers under this option. However, these costs could change depending on Ofcom's final reporting framework.

Finally, Ofcom expects to incur costs associated with monitoring and enforcing industry compliance of £53m - £70m over the impact assessment period. As a result of the Telecommunications (Security) Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, having regard to the code of practice in their regulatory work. The Department for Digital, Culture, Media & Sport (DCMS) will also incur additional costs in providing administrative support for the Secretary of State under the new security regime. These are expected to total £0.9m - £1.4m over the impact assessment period.

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

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

| BENEFITS (£m) | Total Transition (Constant Price) Years | | Average Annual (excl. Transition) (Constant Price) | Total Benefit (Present Value) |
|---|---|---|---|---|
| Low | Optional | | Optional | Optional |

[13] Annex 5: Draft general staement of policy under section 105Y of the Communications Act 2003 - https://www.ofcom.org.uk/__data/assets/pdf_file/0027/233568/annex-5-draft-s105A-Z-procedural-guidance.pdf

| | | | | |
|---|---|---|---|---|
| High | Optional | | Optional | Optional |
| Best Estimate | | | | |

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

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

Estimates suggest that the cost of a security breach or cyber attack for a UK telecoms company could be anywhere in the range of £4,000 to £250m. We estimate that the total central cost over the impact assessment period of security compromises for PECN and PECS providers is £3,300m, within a range of £2,000m - £3,900m. Within this estimate, we have assumed that, over the next ten years, there will be two severe incidents (in line with historic precedent) which reduce the share price of the affected provider, resulting in a loss of £120m per incident. The new security framework will reduce the cost impact of security compromises, reducing the total cost of such compromises. However, we have not estimated the proportion of costs that would be avoided and have therefore not included these benefits in the NPV and EANDCB.

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

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

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

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

At the time of writing this impact assessment, inflation has increased to 9.0% (CPI) in the UK. This is a result of inflation rising by 7.5% over the 12 month period from April 2021. We think that high levels of inflation will likely inflate our final cost and benefits estimates equally. It would be expected that a rise in cost estimates would be driven by increased input costs for telecoms providers e.g. wage and resource costs when complying with the regulations. Furthermore, we think our benefits estimates would be inflated by the costs of avoided security compromises also increasing. As a result, we do not believe inflation will broadly affect our analysis and have used the standard Green Book discount rate of 3.5% for our appraisal.

Due to a lack of available data we were unable to recommend sound upper and lower bound optimism bias levels for our benefits estimates (avoided security compromises and 5G use cases). As an alternative we have used sensitivity analysis to check the plausible range for our estimated benefits.

We have undertaken a 10 year appraisal period as this is a legislative policy, which aligns with Green Book guidance

We have used estimates of costs from providers to estimate the total cost to business of the regulations published in September 2022. There is a risk that the ultimate cost to business once the legislation is implemented may vary from businesses' best estimate at this stage.

It is also the case that:

- We do not know how providers will practically implement the guidance in the code of practice once it is in place or to what degree existing or planned security processes will be in line with the code.
- The code of practice will be reviewed regularly and will be updated as new threats emerge and technologies evolve. Any such review and consultation on changes could affect the costs to business.

**BUSINESS ASSESSMENT (option 2)**

<table>
<tr><td colspan="3">Direct impact on business (Equivalent Annual) £m:</td><td rowspan="2">Score for Business Impact Target (qualifying provisions only) £m:</td></tr>
<tr><td>Costs: 482.7</td><td>Benefits: 0</td><td>Net: 482.7</td></tr>
<tr><td colspan="3"></td><td>2413.6</td></tr>
</table>

# Contents

# Key Terms

| Term | Abbreviation | Available at |
|---|---|---|
| The Telecommunications (Security) Act 2021 *(primary legislation)* | The Act | Legislation.gov.uk |
| The Electronic Communications (Security Measures) Regulations 2022 *(secondary legislation)* | The regulations | DCMS |
| Telecommunications Security Code of Practice | The code of practice | DCMS |
| The Telecommunications (Security) Act including the Electronic Communications (Security Measures) Regulations and the Telecommunications Security Code of Practice | The new security framework | Factsheet on the new telecoms security framework |
| Public electronic communications networks | PECN | Section 151 of the Communications Act 2003 |
| Public electronic communications services | PECS | Section 151 of the Communications Act 2003 |

# 1. Problem under consideration and rationale for intervention

### Policy context

1.1 This document represents the final stage economic assessment of the secondary legislation for the regulations and code of practice. DCMS undertook a secondary stage assessment of the draft regulations and draft code of practice last year. This impact assessment was rated as ‘fit for purpose’ but DCMS have since decided to consult on the proposed measures for the new security framework.

1.2 The initial final impact assessment for primary legislation was approved in August 2020 and fell under scenario 2 whereby the equivalent annual net direct cost to business (EANDCB) was unquantified. As mentioned above, a final impact assessment was then approved in November 2021 with a monetised EANDCB which was validated. In March 2022 a consultation stage impact assessment was then published alongside the formal consultation of the draft regulations and draft code of practice.

1.3 At the time of writing this impact assessment, the key planned changes to the regulations and code of practice following the formal consultation include the following:

- Timelines - DCMS has decided to move the implementation phases to 31 March 2025, 2027 and 2028
- Tiering - telecoms providers who change tier category will be given two years to transition to the new tier requirements
- Scope - clarifications of the terms used to determine the measures as well as greater specificity around some of the measures themselves
- National resilience - greater clarity on the types of services that should be maintained in extremis, and the scenarios where such scenarios would commence
- Legacy networks - greater clarity on the principles to be followed when considering how to apply protections to older 'legacy' networks due to be replaced

1.4 For this impact assessment, the key change for our consideration following the consultation, is in regards to timelines. This has led to an amended cost profiling for one-off and ongoing costs. See the Monetised and non-monetised costs and benefits section for more information.

1.5 Table 1 outlines the key areas the Regulatory Policy Committee (RPC) have outlined for improvement in the previous impact assessments. The table briefly summarises how DCMS has attempted to address these concerns. These areas represent the most pertinent or consistent areas which have been raised by the RPC.

### 1.6 Table 1 - key areas of improvement highlighted in previous opinions

| Area | RPC comment | How we addressed |
|---|---|---|
| Rationale and Options | Final IA needs to discuss assessed options (including impacts) further | • Developed our description of options section<br>• Meetings/ correspondence with providers<br>• Post consultation responses |
| Cost-benefit analysis | The department should seek to strengthen evidence base as much as possible through consultation | • Reissued a new cost survey and took multiple steps to try, albeit unsuccessfully, to get further responses from Tier 3 firms<br>• Meetings/ correspondence with providers |
| EANDCB | Discussion of non monetised impacts e.g. costs passed through e.g. consumers, business customers | • Meetings/ correspondence with providers and discussion now included in IA |
| Monitoring and Evaluation | Include some initial discussion of what metrics could support the evaluation process and what criteria could form the basis for assessing whether the policy has met its objectives | • Discussion with central analysts in DCMS on M&E approach<br>• Engagement with Ofcom on our M&E framework<br>• Collaboration with DCMS analysts who are working on post-implementation review for Network and Information Systems regulations |
| Wider impacts (innovation) | IA would benefit from the inclusion of the expected, or potential, gains to productivity and innovation | • Meetings/ correspondence with providers |
| Wider impacts (competition) | Whether the proposed difference in implementation timescales between options 4 (preferred option) and 5 will have any impact on competition | • Meetings/ correspondence with providers<br>• Post consultation responses |

1.7 Note that the sections highlighted in Table 1 are not the exhaustive list of suggested areas for improvement from previous RPC opinions. Several highlighted areas for improvement were addressed in the final impact assessment at secondary legislation stage last year. In addition, other areas of feedback were most applicable to the consultation stage impact assessment.

**What is the issue being addressed?**

1.8 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.

1.9 These concerns were 'largely related to the overall quality of software engineering, under-investment in cyber security, and a growing dependence on a small number of viable vendors, including high risk vendors.'[14] These were combined with the view that if 5G and full fibre networks are going to deliver significant economic benefits, their deployment must be secure and resilient.

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

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

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

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

**International policy context**

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

- Australia has taken steps in the Telecommunication Security Sector Reforms 2017 (TSSR) to strengthen the requirements for better management of national security risks of espionage, sabotage and foreign interference. Most recently, in 2021, Australia introduced a Security Legislation Amendment (Critical Infrastructure) Bill that amends the Security of Critical Infrastructure Act 2018 to enhance the existing framework for managing risks relating to critical infrastructure.
- India has produced the Telecoms Security and Assurance Requirements (ITSARs) which set out technical measures to protect telecoms equipment and systems.
- The United States has taken steps to improve network and service security by drafting the security guidance for 5G cloud infrastructures which covers wide-ranging guidance to detect and prevent lateral movement, securely isolate network resources, and protect data in relation to 5G networks utilising cloud infrastructures.
- The Netherlands regulation for telecoms security sets out measures that apply to the critical parts of networks. These include safe configuration of technical

[14] UK Telecoms Supply Chain Review Report, paragraph 1.3.

equipment, physical and virtual infrastructure; monitoring of technical infrastructure; and security assurance on software and management services.

- Ireland's Electronic Communication Security Measures set out technical measures that will be given a legislative basis for enforcement.
- Germany has taken steps through the IT Security Act 2.0 (IT-Sig 2.0) which addresses component risks via a two-part assessment mechanism for telecom vendors seeking access to Germany's 5G networks. This enables the German government to ban the use of critical components (including 5G equipment) by telecom providers on the basis of national security.In addition, ban the use of all critical components provided by a manufacturer which has not proven itself to be trustworthy in severe cases. Also, further requirements have been placed through the catalogue of security requirements which covers various potential risks and requires network operators and service providers to meet strict security requirements.

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

**5G and full fibre networks must be secure and resilient**

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

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

1.17 These are set out in Box 1 which is an extract from the Review[15]:

Box 1: 5G networks and security

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

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

[15] UK Telecoms Supply Chain Review Report, paragraphs 2.11 - 2.15.

the security and resilience of the virtualised applications. Given NFVi and MANO will underpin the critical functions of the core, they must comply with the highest levels of security.

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

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

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

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

1.19 This is explained in Box 2 which is an extract from the Review[16]:

Box 2: FTTP networks and security

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

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

*Role of the incumbent.* Unlike mobile networks where there are four national networks, fixed networks have just two incumbent providers in Openreach and KCOM (in Hull)

[16] UK Telecoms Supply Chain Review Report, Paragraphs 2.19 - 2.22.

that together provide national coverage. These incumbents serve several essential functions like alarm systems, telemetry and control systems which will migrate to fibre. As smaller, sub-national, providers build their own market share in the business connectivity market, particularly for critical services, they will need to ensure they are providing the necessary levels of security and resilience.

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

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

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

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

1.22 In January 2020, the NCSC published a report detailing the findings from its extensive analysis of the security of the telecommunications sector[17]. Upon completing the threat analysis, they found that the majority of the highest scoring attack vectors fitted into one of the following five categories:

- Exploitation via the provider's management plane[18]
- Exploitation via the international signalling plane[19]
- Exploitation of virtualised networks
- Exploitation via the supply chain
- Loss of the national capability to operate and secure our networks.

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

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

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

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

1.24 Findings from the UK Cyber Breaches Survey 2020[20] 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.

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

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

- 'Insufficient clarity on the cyber standards and practices that are expected of industry
- Insufficient incentives to internalise the costs and benefits of security. Commercial players are not exposed to the full costs and consequences of security failures; security risks are borne by government, and not industry alone.
- A lack of commercial drivers because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality
- The complexity of delivering, monitoring and enforcing contractual arrangements in relation to security.'[21]

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

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

[20] Cyber Security Breaches Survey 2020: Statistical Release

[21] UK Telecoms Supply Chain Review Report, Page 13.

factors such as cost and quality[22]. The same is true of businesses for example, the Cyber Breach Survey 2020[23] found that only 15% of all businesses surveyed have reviewed the cyber security risks presented by their suppliers.

1.28 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.

1.29 Recent events also strengthen the case for government intervention. In 2018, O2 experienced an outage which left 32.1 million customers without access to the internet[24]. This led to a reduction in both business and personal activities being undertaken via the mobile data network. Furthermore, in 2015 TalkTalk experienced a cyber attack which resulted in the loss of 1.2 million customer's personal data[25]. The likelihood of these events occurring would reduce if greater security duties were placed on providers.

1.30 There is a general consensus that there is a lack of a framework to measure the impacts of cyber attacks. This can make it difficult for key stakeholders to identify the true frequency and magnitude of cyber attacks leading to underreporting. The issue of underreporting is something which has been validated by Ofcom. A stronger framework will provide stakeholders with the necessary information to help measure the true extent of financial and other impacts. Providing the necessary information to all parties will enable those with insufficient knowledge to take the necessary steps to mitigate cyber threats. Therefore, it can be concluded that a stronger framework will help solve issues caused by asymmetric information.

1.31 A lack of understanding of the financial impacts means that some organisations have a reduced ability to identify the types of costs associated from cyber attacks when compared to more cyber security conscious organisations. Additional DCMS research[26] has shown that respondents do not fully count all economic costs, instead focusing on direct financial impacts. As such, the figures are more often than not an underestimate. The issue of asymmetric information may lead to more conscious firms being able to take the necessary steps required to mitigate future cyber attacks when compared to firms that are less aware.

**What sectors/markets/stakeholders will be affected?**

1.32 The Communications Act 2003 places certain responsibilities on providers of PECN and PECS. It defines the terms PECN and PECS in section 151[27].

---

[22]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.

[23] 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.

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

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

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

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

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

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

1.35 In addition to new requirements placed on providers, Ofcom will be impacted through resource requirements to carry out enhanced reporting and oversight duties[28].

**Why is the government best placed to resolve the issue?**

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

1.37 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.

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

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

[28] The impacts on Ofcom have been accounted for in the cost section of this impact assessment: The Telecommunications Security Bill 2020: The Telecoms Security legislation

# 2. Policy objectives

2.1. The objective of the Telecommunications (Security) Act aligns with the DCMS Outcome Delivery Plan[29]. Priority outcome 3 sets out the need to:

- 'increase growth through expanding the use of data and digital technology and increasing innovation
- while minimising digital harms to the UK's economy, security and society'.

2.2. The regulations will support the government in achieving this outcome by providing a security framework to:

- contain unacceptable levels of economic and national security risk in the UK telecommunications sector
- ensure businesses are incentivised to manage telecommunications security risks which will help protect economic activity and consumers
- ensure that public telecommunications providers securely design, construct and manage their networks and services to protect against threats

2.3. The overarching aim of the Telecommunications (Security) Act is that set out in the UK Telecoms Supply Chain Review report, 'to ensure providers of PECN or PECS take appropriate and proportionate measures to prevent, remove or manage the risks posed to the security of networks and services'[30].

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

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

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

[29] DCMS Outcome Deliver Plan: 2021 to 2022

[30] UK Telecoms Supply Chain Review Report, Page 36.

## How will the legislation work?

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

2.7. There are 13 substantive regulations addressing different activities to mitigate threats to networks and services. Each regulation sets out the expected security outcomes and the actions that must be taken to meet them. A summary of each regulation is detailed below in Box 3:

**Box 3 - Summary of the Electronic Communications (Security Measures) Regulations**

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

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

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

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

**Supply chain**
The regulation contains requirements to put appropriate contractual arrangements in place that ensure lifetime product and service security. They also require that written plans are in place in the event that supply from a third party is interrupted. Where a third party supplier given access to sensitive data is another network provider, that provider must take the equivalent steps as the primary provider it is supplying.

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

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

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

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

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

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

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

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

2.8. The Act gives the telecoms regulator, Ofcom, powers to monitor and enforce industry compliance with the duties in the Act and specific security requirements in the regulations. It places new obligations on public telecoms providers to share information with Ofcom that is necessary to assess the security of their networks, including reporting duties in the event of a security compromise.

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

- proactively assess the security practices of telecoms providers;
- take action where security is, or is at risk of being, compromised;
- make information available to the government and, beginning two years after commencement of section 11 of the Act, provide annual security reports to the government

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

2.11. The Act also requires Ofcom to take account of relevant provisions contained in the code of practice when carrying out its compliance activities. Ofcom has consulted publicly on how it intends to use its new powers, including in relation to guidance set out in the code of practice.[31]

**Measuring success of these objectives**

2.12. Measuring success of the policy objectives should be broken down into separate components. Firstly, the success of the regulations should be based against the final monitoring and evaluation framework agreed. The Monitoring and evaluation section below highlights the key data metrics and evaluation options that will be considered when assessing the effectiveness of the regulations.

2.13. Assessing the success of the Telecommunications Security Act should become clearer after the commencement of the regulations and code of practice, when we can confirm whether the new duties for Ofcom help to ensure providers comply with their new duties. Furthermore, confirmation of the powers for the DCMS Secretary of State to issue codes of practice and detailed technical security guidance to assist Ofcom should also be used as a measurement for success.

[31] Annex 5: Draft general statement of policy under section 105Y of the Communications Act 2003, March 2022

# 3. Description of options considered

3.1. The Telecommunications (Security) Act received Royal Assent on 17 November 2021. Once its relevant sections are commenced, it will replace sections 105 A - 105 D of the Communications Act 2003. For option 0 we have considered a counterfactual scenario where the security of telecommunications networks and services are regulated under the Communications Act 2003 as it stood prior to the Telecommunications (Security) Act. The other proposed options are variations of a new telecoms security framework comprising of three layers:

1. **Strengthened overarching security duties set out in primary legislation, via the Telecommunications (Security) Act**. The Act will require providers of PECN and PECS to take appropriate and proportionate measures to identify and reduce the risks of security compromises occurring, as well as preparing for the occurrence of security compromises. It will also require that they take appropriate and proportionate measures to prevent adverse effects from a compromise, and mitigate or remedy any adverse effects.
2. **Specific security regulations set out in secondary legislation, via the Electronic Communications (Security Measures) Regulations.** The Act allows the Secretary of State to make regulations to detail specific security requirements that providers must take.
3. **Codes of practice** - the Act provides the Secretary of State with the power to issue codes of practice to provide guidance on how certain telecoms providers could comply with their legal obligations.

3.2. Telecom providers are assigned into one of three tiers. The tiers are based on relevant turnover over a relevant period of time. The definitions are:

- Tier 1 - public telecoms providers with relevant turnover over a relevant period of £1bn or more.
- Tier 2 - public telecoms providers with relevant turnover over a specified period of more than or equal to £50m but less than £1bn.
- Tier 3 - public telecoms providers whose relevant turnover over a relevant period is less than £50m

3.3. The options we have considered are:

- **Option 0 (Do nothing):** This option involves DCMS taking no action to address the security issues identified in section 1 and retaining the pre-existing obligations in sections 105A to 105D of the Communications Act prior to the Telecommunications (Security) Act coming into force. This is the counterfactual option against which the incremental impact of all other options are considered.

- **Option 1 (the Preferred Option):** The Act places high level security duties on providers, and specific security regulations are set out in secondary legislation. These regulations are applied to providers of communications networks and services (PECN and PECS) in a way that is appropriate and proportionate, reflecting the different characteristics of network security vs service security. A

code of practice is published as best practice guidance for industry to follow and for Ofcom to take into account in ensuring compliance with legal obligations.

- **Option 2 (Implementation plus):** The specific security requirements are set out in the regulations as in the preferred option but implementation of the measures in the code of practice is phased by date only (not by type of provider). This option sets out a single set of implementation dates applying to both Tier 1 and Tier 2 providers.

3.4. The options under examination are option 1 (preferred option) and option 2 (implementation plus) with our counter counterfactual as option 0 (do nothing). Prior to consultation DCMS had 5 options. Following the formal consultation DCMS were able to discount two options which are option 3 (non-regulatory option) and option 4 (guidance issued within the new security framework). Prior analysis stated that guidance does not provide sufficient incentives for telecoms operators to internalise the costs and benefits of security.[32] Therefore the two guidance options as described below were discounted.

- **Option 3 (non-regulatory option):** DCMS works with NCSC and other appropriate industry bodies to produce (non-legally binding) best-practice guidance for telecoms network and service providers.

- **Option 4 (guidance issued within the new security framework):** The Act places high level security duties on providers accompanied by technical guidance, with no further specific regulations set out in secondary legislation. A draft code of practice is consulted on and a final one is published as guidance for industry to follow and for Ofcom to take into account in ensuring compliance with legal obligations.

3.5. Assessments of the extent to which these options meet the government's policy objectives are set out below. These assessments are based on previous analysis and relevant responses to the public consultation on the draft Electronic Communications (Security Measures) Regulations and draft Code of Practice.

**Option 0: The 'Do nothing' option**

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

3.7. We discussed in section 1 the problem under consideration and rationale for intervention. The 'do nothing' option would be to leave the previous existing framework under the Communications Act 2003 in place. However, the UK Telecoms Supply Chain Review found that this was not adequate in addressing the threat assessment and that there were four reasons that the status quo is not sufficient to meet the security needs of the UK's public telecoms networks and services. These are:

[32] The telecommunications security bill 2020

- ‘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.’[33]

3.8. These conclusions were set out in the UK Telecoms Supply Chain Review Report, which was informed by expert technical advice from the NCSC on cyber security considerations, economic analysis from KPMG and discussions with industry and the UK’s international partners. Based on the Review’s conclusions, we assess that option 0 does not meet the security needs of the UK’s public telecoms networks and services.

3.9.

**Option 1: Regulations and Guidance (the Preferred Option)**

3.10. Under the preferred option, the Electronic Communications (Security Measures) Regulations will set out specific security requirements clarifying the priority security outcomes and the strategic actions that must be taken to achieve them. These requirements are intended to apply to all providers of public electronic communications services and networks (PECN and PECS) with a particular focus on network providers, who are responsible for the security of telecoms infrastructure[34]. What this means is that Tier 1 and Tier 2 providers will be required to comply with the mandatory regulations and Tier 3 providers will also be expected to comply to a level which is appropriate and proportionate.

3.11. .

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

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

[33] The Telecoms Supply Chain Review, Page 13.

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

3.13. This overall approach contained in draft regulations and a draft code of practice - including the dates above - were consulted upon between 1 March and 10 May 2022. Of the 38 responses received, 15 respondents agreed with the government's proposals for a new three-layered security framework while three disagreed. Several respondents noted that establishment of a new, rigorous baseline for telecoms security across the industry is necessary, and that they shared the government's goal and approach to achieving these improvements.

**3.14.** We note that 18 respondents did not agree with the government's proposed implementation timeframes for measures in the code of practice. These respondents suggested that meeting the Tier 1 timeframes would be challenging and costly. Following careful reassessment in conjunction with the NCSC, Ministers agreed that additional time for implementation should be given to Tier 1 providers. Analysis in this document therefore assesses expected costs and benefits against the timeframes below:

- **31 March 2024 (Tier 1 only)** - completion of the lowest complexity and least resource-intensive actions
- **31 March 2025** - completion of the remaining low complexity actions achievable with minimal resource allocations for Tier 1; and both the lowest complexity and least resource-intensive actions for Tier 2
- **31 March 2027** - completion of actions which require devotion of new resources and a degree of complexity (Tier 1 and Tier 2)
- **31 March 2028** - completion of high complexity and resource-intensive actions that must take account of wider change programmes or require deeper, strategic solutions (Tier 1 and Tier 2)

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

### Option 2: Regulations and Guidance: Implementation plus

3.16. Under the 'implementation plus' option, the framework would be identical to that proposed by the preferred option. However, this option proposes a single set of implementation timetables for the measures in the code of practice for both Tier 1 and Tier 2 providers. What this means is that Tier 1 and Tier 2 providers will be required to comply with the mandatory regulations and Tier 3 providers will also be expected to comply to a level which is appropriate and proportionate. The proposed implementation dates are:

- **31 March 2023** - proposed completion of the most straightforward actions achievable with minimal resource allocations
- **31 March 2025** - proposed completion of actions which require devotion of new resources and a degree of complexity

- **31 March 2026** - proposed completion of actions that must take account of wider change programmes (such as the PSTN switch-off) or require deeper, strategic solutions.

3.17. The ‘implementation plus’ option differs from option 1 as it sets out a tighter timescale for both Tier 1 and Tier 2 providers.

3.18. As with the implementation timelines highlighted under our preferred option 1, the implementation timeframes under option 2 will also be set out in the code of practice and not in the regulations. The timelines contained within the code of practice will serve as guidance on when the government expects providers to have met their legal obligations, and Ofcom will take account of the code when monitoring compliance with the new framework.

# 4. Rationale and evidence to justify the level of analysis

### Assessing impacts and ensuring proportionality

4.1. DCMS undertook a survey of a sample of providers to understand the cost impacts of the draft Electronic Communications (Security Measures) Regulations which was launched in March 2022. This survey superseded a previous survey that DCMS issued to understand the impacts of an earlier illustrative draft version of the regulations, which was published in January 2021.

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

4.3. We issued a detailed survey on 1 March 2022 to a number of the larger providers. It was a structured set of around 90 questions asking providers for information on the changes required to implement the new security requirements and the ongoing and one-off costs of implementation for each section of the draft regulations. It also included questions on familiarisation costs, method of compliance and potential benefits of the legislation.

4.4. The survey asked for the costs of compliance with the draft Electronic Communications (Security Measures) Regulations published on 1 March 2022, taking into account the draft code of practice that was also published on 1 March 2022. Respondents were able to access the draft regulations and the draft code of practice from the GOV.uk website.

4.5. For smaller providers, DCMS issued the same length survey of around 90 questions on 1 March 2022 This survey asked for overarching one-off and ongoing costs of implementation. It also asked about the cost impacts per section of the regulation which respondents were able to skip due to the resources needed to quantify these costs. It also included questions on the degree of current compliance, familiarisation costs and potential benefits of the legislation.

4.6. DCMS issued both surveys via the online portal, Qualtrics, while also sending the cost survey directly to over 250 telecoms providers. The cost survey was also communicated to telecoms providers through the UK's trade body for internet service providers, the Internet Service Providers' Association (ISPA), and the Federation of Communications Services (FCS).

4.7. DCMS received 15 responses to the survey in total. DCMS received 7 responses from the providers expected to fall into Tier 1 (100% of the sample size), 4 responses from those expected to fall into Tier 2 (13% of the estimated sample size) and 4 responses from those expected to fall into Tier 3 (approximately 1% of the estimated sample size). In order to better understand how representative, the sample is, DCMS asked questions regarding the type of provider and primary industry classification and compared this to the available data on PECS and PECN providers. DCMS used the output on costs as a proportion of turnover to estimate the potential scale of impact on all providers subject to the regulations, taking the type of provider into account.

4.8. The surveys were issued on the same day that the draft regulations and code of practice were published, alongside a consultation document seeking views on particular aspects of both. Providers were given an initial six weeks to respond to the survey. A two week extension was added to the deadline in an attempt to obtain more survey responses.

4.9. Clarification interviews were undertaken by DCMS analysts after the survey closed to seek further clarification from providers on particular points in their responses or where their responses raised additional questions (such as citing significantly different costs to those given by similar providers). DCMS contacted 8 providers and 4 agreed to be interviewed, which were attended by a DCMS technical adviser to help validate the responses where needed. DCMS received further qualitative evidence via email from one other provider.

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

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

4.11. The Telecommunications (Security) Act requires government to consult with Ofcom and providers of PECN/S before issuing a code of practice[35]. This will ensure that codes of practice are targeted and proportionate, by taking into account the views of the businesses that may seek to follow guidance measures. Given the need to ensure appropriate and proportionate secondary legislation for the initial implementation of the new framework, the first consultation launched in March 2022 was extended to include the regulations.

4.12. Since the Act was first introduced to Parliament in November 2020, DCMS has been engaging consistently with industry on the contents and impact of the proposed regulations and code of practice. The timeline of engagement is below.

- November 2020 - present (ongoing): DCMS has held bilateral engagement with individual telecoms providers, suppliers and trade bodies to clarify impacts of proposals and understand how they would meet the security intent. This information fed back into the policy decisions put to Ministers to ensure the contents of the regulations and code of practice are balanced and proportionate.
- November 2020 - December 2021: DCMS held monthly industry forums to update on passage of the Act and next steps, and answer questions from industry. The forums included providers of all sizes and functions, as well as suppliers and cross-sectoral representative bodies, reflecting the full breadth of the UK's telecoms market.
- January 2021: DCMS published an early draft of illustrative draft regulations. This was accompanied by an open call for technical feedback, lasting four weeks from the publication. A cost survey was also carried out in relation to the illustrative draft.
- March - May 2021: DCMS held technical roundtable sessions with providers of all sizes and functions, as well as suppliers and cross-sectoral representative bodies,

[35] Communications Act 2003, s.105F (as amended by the Telecommunications (Security) Act 2021)

reflecting the full breadth of the UK's telecoms market. This engagement gave telecoms providers and other affected parties an opportunity to comment on the technical guidance measures that would be included in a draft code of practice, helping to ensure guidance measures are proportionate and operationally realistic.

- 1 March 2022: DCMS held a consultation launch event with attendees of the monthly industry forum. This explained the consultation format, the contents of updated draft regulations and the new draft code of practice, and process for engagement while consultation was ongoing.
- 1 March - 26 April 2022: DCMS issued a cost survey to a representative sample of affected public telecoms providers to seek feedback on business impacts of the draft regulations.
- 1 March - 10 May 2022: Public consultation on draft Electronic Communications (Security Measures) Regulations and draft Telecommunications Code of Practice.

4.13. DCMS has also considered the need to reflect the differences in scale and criticality of providers' networks and services. Micro-businesses will be exempt from the Electronic Communications (Security Measures) Regulations.[36] If applied to them, the legislation could have a disproportionate financial impact on micro businesses, whose networks and services present much less risk to UK connectivity. The disproportionate financial impact on micro-businesses would primarily come from higher relative fixed costs, limited in-house technical expertise and higher relative familiarisation costs.

4.14. For the remaining non-micro businesses impacted by the regulations and code of practice, DCMS has implemented a system of tiering set out in the code of practice. Details on this are set out in section Description of options considered above. The use of a tiering system will enable differences among providers to be reflected in the new framework, and should ensure security measures are applied appropriately and proportionately.

4.15. Finally, the new legal obligations on providers will be overseen and enforced by Ofcom. In performing its duties, Ofcom must have regard, in all cases, to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed. Ofcom will also take into account the provisions contained in the code of practice, including the tiering system for providers. Ofcom has consulted on its proposed procedural guidance setting out how it intends to apply a proportionate approach to using its new powers[37].

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

[37] Annex 5: Draft general statement of policy under section 105Y of the Communications Act 2003, March 2022

# 5. Preferred option with description of implementation plan

### How will the preferred option be given effect?

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

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

5.2. The Electronic Communications (Security Measures) Regulations 2022 contain the specific security requirements, under the second layer of this framework. The Telecommunications Security Code of Practice contains technical security measures as guidance, under the third layer of the framework. Both documents are published alongside this impact assessment.

### What will legislation seek to do?

5.3. The Electronic Communications (Security Measures) Regulations include targeted actions to ensure that public telecommunications providers take such measures as are appropriate and proportionate for the purposes of:

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

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

5.5. The government is also laying commencement regulations alongside the Electronic Communications (Security Measures) Regulations, to bring the new security framework into effect from 1 October 2022. The commencement regulations bring into effect the Electronic Communications (Security Measures) Regulations, the remainder of the provisions in clauses 1 to 13 of the Act that were not commenced on Royal Assent, and the code of practice. This ensures that formal commencement is in line with a fixed point in the financial year, to assist business decision making.

### Does the approach to implementation enable sufficient flexibility?

5.6. The new telecoms security framework has been designed to balance certainty and clarity to providers on achieving good security with the flexibility to update requirements and guidance measures as threats emerge and technologies evolve. The regulations

will be reviewed in a Post Implementation Review which will take place in 2027. They may be updated on a more regular basis to reflect changes in policy in response to the emergence of specific new threats or to address security vulnerabilities identified through compliance reporting. The code of practice will be reviewed regularly and will be updated as new threats and vulnerabilities emerge and technologies evolve. The framework allows for providers to take their own actions to improve security rather than follow the code of practice, provided they can demonstrate to Ofcom that they continue to meet their legal obligations. This ensures flexibility for innovation and lets providers secure networks and services in ways that are appropriate to them. Based on the responses to the cost impacts survey, we anticipate that providers will use this flexibility based on our survey of PECN and PECS. In particular, we found 80% of those that responded said they would comply 'By implementing the requirements set out in the draft code of practice where possible but for some areas we will set out our own approach' The remaining respondents indicated that they would adopt the requirements as set out in the draft code of practice. When asked for the reason for their approach the joint most popular responses were 'to maximise network security', 'to maximise chances of full compliance' and 'to ensure a standardised approach with other operators'.

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

## Limitations of the calculations and estimates

6.1. While this impact assessment brings together evidence from a number of sources, we would like to note there are a number of limitations to the cost analysis. The costs are based on responses to a survey issued by DCMS, which was largely disseminated through relevant trade bodies and directly issued to over 250 telecoms providers. For this reason, the process was not random and the sample is therefore unlikely to be representative.

6.2. In particular, there was a much higher response rate among the largest providers (those expected to fall into Tiers 1 and 2) than smaller providers (those expected to fall into Tier 3)[38]. The response rate compared to the estimated population is shown in Table 2.

**Table 2: DCMS cost impact survey response rate by Tier**

| | Estimated response rate |
|---|---|
| Tier 1 | 100% |
| Tier 2 | 13% |
| Tier 3 | 1% |

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

- There is likely to be a selection bias whereby those providers who responded are the providers who are incurring the highest costs.
- This is innovative legislation and providers may face uncertainty in estimating the costs they will incur. Some cost figures provided in the survey were caveated with the respondent noting this uncertainty.
    - A small number of providers have not provided costs for all sections of the regulation. Those providers may not have been able to fully quantify the costs from implementing the regulation and code of practice.
- A number of questions in the survey asked respondents to select a cost range. Since the cost ranges provided were wide (e.g. £25m-£75m), the cost analysis in this impact assessment offers a wide gap between the low and high estimates.
- We acknowledge we have received a low response rate from Tier 3 providers. To mitigate this issue we estimate the impacts by using proxy data, based on the data we collected as well as sensitivity analysis.

6.4. Additionally, during the time of the survey being issued there remained some

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

uncertainties around the code(s) of practice which gives rise to shortcomings in the analysis:

- When we carried out the cost survey we were also consulting on the implementation timescales for the code of practice and these are likely to be a key driver of costs.
- The code of practice will be reviewed regularly and will be updated as new threats emerge and technologies evolve. Any such review could affect the costs to business.

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

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

6.7. The low response rate from Tier 2 providers was unexpected as the detail in the code of practice will be relevant to these providers when meeting the regulations. There are some possible explanations for this outcome:

- Firstly, the cost survey was issued in parallel to other government engagements with industry including the Designated Vendor Direction (high risk vendor) consultation and DCMS' formal consultation with industry on the draft regulations and draft code of practice. This suggests Tier 2 providers may have been resource constrained with multiple ongoing consultations. To mitigate this issue DCMS extended the cost survey deadline by two weeks.
- Secondly, the variation in size across Tier 2 providers is wide, which could imply that smaller Tier 2 providers do not think the regulations and code of practice will significantly impact their business.

6.8. The low response rate from Tier 3 providers is consistent with what we observed during last year's cost survey for the early draft regulations and draft code of practice. This is despite the department's efforts to increase Tier 3 engagement from last year by:

- undertaking a separate telecoms market research project to better understand the demographics of the telecommunications sector.
    i. The project resulted in over 250 contact details of telecoms providers (predominantly smaller providers) who agreed to being recontacted and consequently received a direct link to this year's Electronic Communications (Security Measures) Regulations cost survey.

- extending the initial cost survey deadline by an additional 2 weeks after the low response rate following the initial deadline.
    i. Notice of the cost survey deadline extension was communicated directly to telecoms providers using the contact details we had collected.

ii. Notice of the cost survey extension was also communicated through numerous trade bodies and organisations including ISPA, Mobile UK, TechUK, INCA, UKCTA and others

- attempting to arrange clarification meetings with Tier 3 providers following the deadline of the cost survey to gain further qualitative evidence of the impact of the regulations and code of practice on Tier 3 providers. The response rate to these meetings was 50% across all providers, however we were unable to schedule meetings with any Tier 3 providers despite our efforts to do so.

6.9. DCMS believes there are a few reasons for the consistently low engagement from Tier 3 providers. Firstly, the low response rate suggests a lack of engagement with the regulations and its associated impacts, with some Tier 3 providers possibly believing that the new legislations do not directly apply to them. Our view that the regulations and code of practice will not have a disproportionately large impact on Tier 3 providers supports this point. It is true that there are a wide variety of companies within Tier 3 and some will be impacted far more than others. Some providers offer local telecoms networks and thus will be affected by a number of the regulations; others simply package and sell third-party services, so are only tangentially impacted by the regulations. Some provide telecoms services as their primary activity; others provide telecoms services as a small proportion of their total operation. Finally, it may be the case that some Tier 3 providers lacked the capacity to respond to our cost survey, with smaller providers less likely to have dedicated compliance teams available to support a response to the survey. As a result of the limited survey response from Tier 3 providers, note that we have relatively low confidence that these estimates are an accurate representation of the true costs incurred by such providers.

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

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

### The costs and benefits of the proposed approach

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

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

### What is the counterfactual?

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

6.14. Sections 105 A-D of the Act cover the '*Security of public electronic communications networks and services*'[39]. Section 105A sets out the following four requirements to protect security of networks and services:

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

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

[39] Communications Act 2003, Section 105.

## Economic impact - costs

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

### Number of businesses that will be affected

6.17. The security requirements set out in the regulations apply to all public telecommunications providers except those who are classified as micro-businesses, whose scale poses much less risk to UK connectivity[40].

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

- **Tier 1**, public telecoms providers with relevant turnover over a specified period of £1bn or more. This should be those where a security compromise has the most widespread availability impact, and damaging security, economic or social effects[41].
- **Tier 2**, public telecoms providers with relevant turnover over a specified of more than or equal to £50m but less than £1bn. These should be those medium sized companies whose compromise would nevertheless impact critical sector or regional availability with potentially significant security, economic or social effects.
- **Tier 3,** public telecoms providers whose relevant turnover over a specified period is less than £50m. These should be the smallest companies in the market that are not micro businesses. While security compromises could damage end-user customers, small businesses who do not support CNI do not present systemic risks to national, regional or critical sector availability.

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

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

- There were 123 providers who paid administrative fees to Ofcom and therefore have a relevant turnover of over £5m in 2020/21[42]

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

[41] The latter description of the type of provider this includes, based on the impact of security compromises, is not the formal definition of providers by tiers in this document and is a separate definition

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

- There were 193 providers who had applied for Code Powers[43] under the Electronic Communications Code and are therefore on Ofcom's 'register of persons with powers under the Electronic Communications Code' on 12 November 2020[44]
- There were 596 providers who had telephone numbers allocated to them under Ofcom's Number Management System on 12 November 2020[45]

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

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

6.23. As a result, it is difficult to confidently estimate the precise number of telecoms providers that will be in scope of the regulations and code of practice. Based on data provided by Ofcom, data underpinning last year's impact assessment (secondary legislation) and a telecoms market research project undertaken by DCMS (see below), we have estimated the approximate number of businesses in scope of this legislation to be 450. This number is the estimate we have used throughout our cost-benefit analysis. This estimate aligns with the values displayed in Table 18 (excluding micro-businesses). Note, that Table 18 categorises telecoms providers by employee numbers, while our analysis split businesses by tiers based on relevant turnover.

6.24. As mentioned above, in December 2021 DCMS carried out a market research survey to help further understand and classify the types of providers of telecommunications networks and/or services in the UK. This included understanding more about the number of telecoms providers operating in the UK including their size, activities of companies providing electronic telecommunications networks and services as well as the segments they operate in and their expected growth[46]. Below are the key findings from the research survey:

- A sample of 450 companies completed the market research survey. These companies were identified as providing an Electronic Communication Network, Electronic Communication Service or Associated Facility Service.
  i. 66% of companies were classified as micro (0-9 employees),
  ii. 25% of companies were classified as small (10-49 employees),
  iii. 7% of companies were classified as medium (50-249 employees) and

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

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

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

[46] The survey commenced on 1st December 2021 and ended on 3rd February 2022.

iv. 2% of companies were classified as large (250+ employees).

- Classification breakdown:
  i. 43% provide an electronic communications service,
  ii. 18% provide an electronic communications network,
  iii. 19% provide an associated facility and
  iv. 21% provide more than one of the services (multiple options selected)

- Over a third of respondents provide both a public and private network. Breakdown provided below:
  i. 33% provide a private network[47]
  ii. 25% provide a public network[48]
  iii. 38% provide both and
  iv. 4% selected other (free type)

- Almost three quarters of respondents expect growth over the next 5 years. When prompted on why decision makers believe their business will increase, they provided generalised answers like 'returning to pre-pandemic levels of growth, focusing on the telecoms area and investing in core networks' etc. Whereas, when prompted on why they believe their business will decrease or stay the same, decision makers gave more precise answers like 'lack of investment to expand, covid aftershocks, market shrinking and having no desire to grow further due to being content with the size of company' etc. Breakdown provided below:
  i. 72% of respondents anticipate increase in business growth,
  ii. 4% of respondents expect to see a decrease in business growth,
  iii. 22% of respondents expect their growth to stay the same and
  iv. 1% of respondents were not sure.

- Over a half of respondents are aware of the Telecommunications (Security) Act. Breakdown by size:
  i. 55% of micro companies are aware of the Act,
  ii. 62% of small companies are aware of the Act,
  iii. 67% of medium companies are aware of the Act and
  iv. 78% of large companies are aware of the Act

6.25. Some of the results from this market research project have been used to inform the analysis in this impact assessment. The findings from the market research project will be published alongside this impact assessment.

[47] A private network is a network that is not publicly available but provided in ways that are agreed through a negotiated contract between the seller and buyer. Communications networks provided to airports and hospitals would be some examples of private networks.

[48] A public network is an electronic communications network that is available off the shelf to members of the public including consumers and businesses. These include leased lines as well as broadband networks that provide connections to residential homes.

### Type of businesses that will be affected

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

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

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

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

6.29. The new security framework will not directly apply to equipment vendors or managed service providers, though these entities will be impacted indirectly via new obligations on PECN and PECS providers to secure their supply chains[49].

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

### Direct costs

6.31. Direct costs are those which fall upon those directly accountable for compliance, are immediate and unavoidable ('first round') and are in the market being regulated.[50] Indirect costs are those costs that are not direct. This distinction is important because direct costs form the score for Business Impact Target and the metric 'Direct Costs to Business (Equivalent Annual)'. The following sections detail the direct costs to industry, Ofcom and DCMS. The costs incurred by industry are split into familiarisation costs, one-off and ongoing costs and compliance and reporting costs. The costs incurred by Ofcom and DCMS are detailed in the section entitled 'Monitoring costs'.

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

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

**Familiarisation costs**

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

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

6.34. To gain a better understanding of the impact from the regulations on affected businesses, providers were invited to complete a survey. This survey ran from 1 March to 26 April 2022. The survey received 7 responses from the providers expected to fall into Tier 1 (100% of the sample size), 4 responses from those expected to fall into Tier 2 (13% of the estimated sample size) and 4 responses from those expected to fall into Tier 3 (approximately 1% of the estimated sample size). The survey collected information on company turnover, familiarisation costs, as well as business activities associated with complying with individual sections of the draft regulations. These sections included network architecture, protection of data and network functions, protection of certain tools enabling monitoring or analysis, monitoring and analysis, supply chain, prevention of unauthorised access or interference, remediation and recovery, governance, reviews, patches and updates, competency, testing and assistance. .

6.35. In order to estimate these familiarisation costs, we asked survey respondents to estimate what costs they will incur as a result of familiarisation (defined as the costs of reading and understanding new/amended regulatory requirements and guidance) in relation to both the draft regulations and draft code of practice. To ensure a more accurate assessment of familiarisation costs, the department amended this year's survey to include a broader range for familiarisation hours following feedback from providers who responded to last year's cost survey which ran from 29 January to 12 March 2021[51]. We also followed up respondents' answers in clarification interviews to understand whether the familiarisation costs estimated include substantial dissemination and training costs.

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

6.37. The largest providers (those expected to fall into Tier 1) stated an average familiarisation cost of approximately 930 hours with the source of these cost hours distributed across legal (30%), operational (36%) and other (34%). Those respondents expected to fall into Tier 2 estimated an average familiarisation cost of approximately 670 hours with the source of these cost hours distributed across legal (20%), operational (37%) and other (43%). We consider that familiarisation costs for Tier 2 providers without code powers may be lower than for providers with code powers, given

[51] Previously, the business impact cost survey familiarisation hours range was limited to a maximum of 200 hours for all three breakdowns (legal, operational and other). This year the maximum range is 400 hours.

that providers without code powers are likely to be providers of communication services (PECS) only. Not all sections of the draft regulations and draft code of practice apply to PECS providers. Therefore, we do not expect these providers to spend the same amount of time familiarising themselves with the legislation as those providers with code powers, to whom the regulations and code of practice are likely to apply to in full. However, we do not have clear evidence to support this assumption, so in our cost model we have assumed costs to be the same across providers with and without code powers. Costs for all Tier 2 providers were driven by operational and other job functions.

6.38. Smaller providers (those expected to fall into Tier 3) provided an average familiarisation cost of 410 hours with the source of these cost hours distributed across legal (20%), operational (53%) and other (27%). Again, we assume that all providers incur the same familiarisation costs. We also note that the sample size for respondents in Tier 3 is low; however, as the findings are not dissimilar from the results for Tier 2 providers we retain them as a best estimate.

6.39. The wages for information technology and telecommunications directors are taken from the ONS' Annual Survey of Hours and Earnings[52]. The median is used as a best estimate, as it is believed to be the most representative wage (it is less skewed by outliers).

**Table 3: Wage per hour: Annual Survey of Hours and Earnings (2021)**

| | Hourly wage rate | Hours | Total wage cost | Total wage cost with 22% uplift for overheads |
|---|---|---|---|---|
| Job Title | Median | | £ GBP | £ GBP |
| Tier 1 providers | | | | |
| Legal | 26.60 | 240 - 310 | 6500 - 8400 | 7900 - 10200 |
| Operational (e.g. IT or network functions) | 24.81 | 320 - 350 | 7800 - 8700 | 9600 - 10600 |
| Other [53] | 24.95 | 290 - 350 | 7200 - 8700 | 8700 - 10700 |
| Total | - | 850 - 1010 | 21500 - 25800 | 26200 - 31500 |
| Tier 2 providers | | | | |
| Legal | 26.60 | 90 - 180 | 2300 - 4700 | 2800 - 5700 |

[52] ONS, Annual Survey of Hours and Earnings - Occupation SOC10 (4) Table 15.5a Hourly pay - Gross 2021.

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

| | | | | |
|---|---|---|---|---|
| Operational (e.g. IT or network functions) | 24.81 | 200 - 300 | 5000 - 7400 | 6100 - 9100 |
| Other | 24.95 | 230 - 330 | 5800 - 8300 | 7100 - 10100 |
| Total | - | 520 - 810 | 13100 - 20400 | 16000 - 25000 |
| Tier 3 providers | | | | |
| Legal | 26.60 | 50 - 110 | 1400 - 3000 | 1700 - 3700 |
| Operational (e.g. IT or network functions) | 24.81 | 180 - 260 | 4400 - 6500 | 5400 - 7900 |
| Other | 24.95 | 70 - 150 | 1700 - 3700 | 2100 - 4600 |
| Total | - | 300 - 520 | 7500 - 13200 | 9200 - 16200 |

6.40. Overhead charges of 22% are added to the wages, in accordance with Regulatory Policy Committee guidance on implementation costs[54] which uses Eurostat data on UK non-wage and wage costs to calculate this uplift.

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

- £26,200 - 31,500 per Tier 1 provider.
- £16,000 - 25,000 per Tier 2 provider.
- £9,200 - 16,200 per Tier 3 provider.

6.42. We have tested these estimates using speed of reading estimates produced by Eftec[55] which finds that the average speed of reading a technical text is 50-100 words per minute. The draft statutory instrument which sets out the duties on providers at secondary legislation is approximately 2,500 words and the draft code of practice is roughly 22,000 words. Based on this, the average time spent reading the secondary legislation and draft code of practice is between 4 and 8 hours per person.

6.43. Based on 8 hours per person, the 930 hours of familiarisation time given by Tier 1 providers suggests that, on average, 116 people in each Tier 1 business will be reading the documentation. For Tier 2 providers with code powers, the estimate of 670 hours suggests 84 people will be reading the relevant documentation. These numbers approximately reflect anecdotal feedback given to DCMS about the number of persons reading the regulations in bilateral conversations with larger telecommunications providers in June 2020.

6.44. For Tier 3 providers with code powers, the 410hours estimate translates into 51 people reading the documentation. This is highly likely to be an overestimation as many Tier 3 providers are small businesses with less than 50 employees. However, smaller providers may require external input in reading and understanding the regulations where they lack internal expertise and this might imply higher wages per hour. We have

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

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

therefore retained the estimate as it is. In addition, for the latest cost survey we increased the upper bound for familiarisation hours from 200 hours (last year) to 400 hours following feedback from telecoms providers. We believe this will adequately capture additional costs smaller providers may incur to hire external professionals to help them understand and implement the regulations and code of practice. We note that the average familiarisation hour estimates this year were higher across all tiers when compared to last year's survey results.

6.45. We assume that familiarisation costs will be incurred during 2022 and 2023. We have used a two year cost period as opposed to the standard first year only, due to the extended, phased implementation of the regulations from the years 2022 - 2028. The total estimated familiarisation costs incurred by all providers over the impact assessment period is shown in table 4.

**Table 4: Total familiarisation costs for all providers**

| Familiarisation costs in net present value terms over period 2022-31, £m | |
|---|---|
| Central estimate | 6.2 |
| Low estimate | 4.6 |
| High estimate | 7.8 |

6.46. Whilst our survey clearly defined familiarisation costs[56], during the clarification interviews we noted that the scope of familiarisation costs was wide. Due to the complexity of the regulations and the size of some affected businesses the costs of dissemination and training were interlinked with familiarisation and likely created an upward bias which would make our final cost estimates conservative.

**Options Analysis: Familiarisation costs**

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

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

6.49. The draft statutory instrument which sets out the duties on providers at secondary legislation is approximately 2,500 words and the draft code of practice is roughly 22,000 words. Based on this, the average time spent reading the secondary legislation and draft code of practice is between 4 and 8 hours per person; using speed of reading estimates produced by Eftec[57] which finds that the average speed of reading a technical text is 50-100 words per minute.

6.50. However, the number of people reading and understanding the regulations and code of practice will also be a key driver of familiarisation costs. Our current estimates indicate

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

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

that on average 100 - 120 people within a larger operator will read and understand the regulations and code of practice.

## One-off and Ongoing costs

### Survey Approach

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

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

6.52. As detailed in the section above Rationale and evidence to justify the level of analysis, the survey responses provide us with a view of the scale of the changes that providers need to make to implement the regulations. The responses also inform our estimates for the costs incurred by providers as a result of such changes.

6.53. The survey split these costs into one-off implementation costs and annual ongoing costs, so we have separated these costs in the following analysis. One-off costs are the upfront costs that providers will incur in implementing the initial changes. Examples of one-off costs include the costs of re-architecting networks, moving critical functions to the UK, negotiating contracts with suppliers and deploying privileged access workstations. Ongoing costs are the costs that providers will continue to incur once the necessary changes are implemented. Examples include costs of regular security patching, ongoing storage of data, provision of regular training to staff and increasing permanent headcount to meet monitoring and audit requirements.

### Survey Methodologies

6.54. The cost estimates provided by industry in the cost impact survey have been produced using a range of methods. Some providers noted this methodology in the initial survey response, with some undertaking gap analysis to assess the impact of the draft regulations on their business,

6.55. The previous survey did not include a question on the methodologies used to produce cost estimates so we did not have a full picture of how providers reached their cost estimates. In this year's survey (March 2022), we included a question on the methodologies used. This helped us understand the assumptions used for the cost estimates before we conducted clarification interviews to gain further information on telecom providers responses.

### Survey parameters

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

- refer to a version of the draft regulations published in March 2022
- have read and understood the NCSC's draft telecoms security guidance (larger providers only)

### Costs incurred by Tier 1 and Tier 2 providers

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

6.58. The survey asked for the costs of compliance with the draft Electronic Communications (Security Measures) Regulations and draft code of practice published on 01 March 2022. We received 11 responses from larger companies, whom we expect to fall into Tiers 1 and 2. We estimate that this sample constitutes approximately 30% of all companies that will fall into these Tiers.

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

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

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

6.61. For Tier 2 providers, around 13% of the estimated total population provided a response to the survey. In order to estimate the costs across all Tier 2 companies, we have used the costs provided by the largest providers (those expected to fall into Tiers 1 and 2)[58] to estimate the median[59] cost as a percentage of a total turnover. We used this approach to account for the fact that the costs incurred are likely to increase with the size of the company (an assumption which is backed up by the survey responses). We estimated the total turnover for the entire Tier 2 population based on data from FAME, a company information database from Moody's Analytics[60].

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

### One off and ongoing costs: by business type

6.63. As set out in the section 'Number and type of businesses that will be affected', we have used the list of providers with code powers as a proxy for those providers who own or operate network infrastructure.

6.64. The majority of the respondents to our survey hold Code Powers including all of the providers in Tier 1 and Tier 2. However, comparing the providers likely to fall into Tier 2 with the providers with code powers, we estimate that around 40% of those providers that will fall into Tier 2 do not hold code powers. This estimate was based on Ofcom's

[58] The cost as a percentage of turnover for Tier 1 and 2 is used because the sample size for Tier 2 alone is small and there exists a substantial variation between responses. The variation of size of company (relevant turnover) within the Tier 2 category is also large. Including Tier 1 responses produces a more stable estimate.

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

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

'register of persons with powers under the Electronics Communications Code[61]' as well as last year's cost survey analysis. Similar to last year we received a low number of responses from providers without code powers. This year, all Tier 1 and Tier 2 respondents had code powers. We have remained consistent with last year's impact assessment by assuming providers without code powers are more likely to incur lower than average costs.

**Survey results**

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

6.66. To estimate the costs of the companies we expect to fall into Tier 2, we have calculated the median cost as a percentage of turnover incurred by survey respondents. We then estimated the total turnover of those Tier 2 providers with code powers using turnover data from FAME, and applied the median cost as a percentage of turnover to this total. When estimating the costs incurred by providers who do not have code powers, we have assumed those providers will incur 25% of the costs incurred by providers with code powers. This assumption[62] is based on last year's survey responses from Tier 2 providers without code powers as well as the response we received from a provider without code powers this year. We believe that this is a conservative estimate.

6.67. We have assumed one-off costs for Tier 1 providers are incurred evenly over the years 2022 - 2027 (inclusive). For Tier 2 providers we assume that one-off costs are spread evenly from the years 2023 - 2027 (inclusive). This aligns with the proposed implementation timeframe, for our preferred option' outlined in the 'Description of options considered' section and is supported by the qualitative feedback we received from telecoms providers. The deadlines for implementation of the different parts of the measures is phased from March 2024 to March 2028. In our central scenario, we have conservatively assumed ongoing costs for Tier 1 providers will commence from the year 2022 onwards with only half of the annual ongoing cost incurred in year 1 due to the legislation commencing part way through the year. We have also assumed that Tier 2 providers will start incurring ongoing costs from 2023 onwards with only half of the cost incurred in year 1 due the legislation commencing part way. In the low case, we have assumed ongoing costs are incurred a year later for Tier 1 (October 2023) and Tier 2 providers (October 2024). Again assuming half cost in the first year of the expense occurring and full cost thereafter.

[61] Ofcom's register of persons with powers under the Electronics Communications Code - May 2022

[62] 25% was a conservative figure chosen as our best guess for the proportion of costs incurred by providers without code powers compared to those with code powers. Further information has been provided to the RPC in a confidential note.

6.68. The results are shown in Table 5 below.

**Table 5: Total one-off costs[63] and ongoing costs[64] for Tier 1 and Tier 2 providers**

| | Total costs in net present value terms over the period 2022 - 2031 (3.5% discount rate), £m | | |
|---|---|---|---|
| | Low estimate | Central estimate | High estimate |
| One-off implementation costs | 1000 | 1710 | 2400 |
| Annual ongoing costs | 100 | 180 | 240 |
| **Total costs incurred** | **1990** | **3470** | **4780** |

6.69. We estimate a wide range of costs from a low of £2.0bn to a high of £4.8bn . This range reflects the format of our survey which asked respondents to indicate their costs within broad ranges. This approach was based on an assumption that respondents would find it difficult to provide a point estimate of costs impacts. This approach was also supported by our qualitative interviews where respondents noted that there is a wide degree of variance in their estimates and in many cases that they did not have a point estimate for their costs and were only able to indicate the range of costs.

6.70. Our central estimate is the midpoint of the low and high cases[65]. The survey asked respondents to select a cost range; the lower bound informed our low estimate and the higher bound informed our high estimate. In order to better understand the estimates provided in the survey, we used the follow up interviews to ask where their actual costs lay within this range. The majority of providers suggested they did not know where their costs would fall within the range chosen and we consider that there could be a high level variance from their estimates to the true costs. Many noted that there was a high level of uncertainty in the costs they expect to incur. One Tier 1 provider did note that if they had the resources to implement all changes from the requirements at once they would anticipate a lower overall cost compared to addressing each section of the regulation separately as they may need to continuously retrofit. In the absence of any further quantitative evidence, we have used the midpoint of the survey responses as the central estimate.

6.71. For Tier 2 providers we have considered whether selection bias means that those providers that responded were those that would incur proportionately more costs.

[63] We have assumed one-off costs for Tier 1 providers are incurred evenly over the years 2022 - 2027. For Tier 2 providers we assume that one-off costs are spread evenly from the years 2023 - 2027. .

[64] In our central scenario, we have conservatively assumed ongoing costs for Tier 1 providers will commence from the year 2022 onwards with only half of the annual ongoing cost incurred in year 1 due to the legislation commencing part way through the year. We have also assumed that Tier 2 providers will start incurring ongoing costs from 2023 onwards with only half of the cost incurred in year 1 due the legislation commencing part way. In the low case, we have assumed ongoing costs are incurred a year later for Tier 1 (October 2023) and Tier 2 providers (October 2024). Again assuming half cost in the first year of the expense occurring and full cost thereafter.

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

However, our assumption that providers with code powers will incur higher costs should reduce any potential selection bias. Therefore, we retain the midpoint as our central estimate.

6.72. Our central estimate gives a total cost incurred by Tier 1 and 2 providers of **£3.5bn** over the next ten years in net present value terms. This is based on Tier 1 providers incurring one off costs over the years 2022 to 2027 and ongoing costs from October 2022 onwards. We assume that Tier 2 providers will spread one-off costs from 2023 to 2027 and incur ongoing costs from 2023 onwards.

6.73. We have conducted some sensitivity analysis on these costs to illustrate the impact of varying our assumptions. In a high cost scenario, we use the mean cost as a percentage of turnover given in the survey, rather than the median, to estimate the costs to Tier 2 providers who have not responded to the survey. The turnover and code power assumptions for providers remain unchanged. In this scenario, our central estimate gives a total cost incurred by Tier 1 and 2 providers of **£3.9bn** over the next ten years in net present value terms.

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

**Range of Estimates**

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

6.76. For Tier 1 providers, all responses produced an estimate of one off costs ranging between 0.2-12% of annual turnover, with most responses falling between 2 - 5% of annual turnover. There is less variation in the ongoing costs as a percentage of turnover. The range of central estimates is 0.08% - 1.3% of annual turnover, with most costs falling between 0.3% - 0.7% of annual turnover.

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

- Different interpretations of certain requirements within the regulations and the code of practice. A number of differing interpretations have been identified in follow-up interviews led by DCMS and technical reviews led by NCSC. DCMS and NCSC are working with industry to clarify these areas of uncertainty.
- Different interpretations of survey questions.
- Nature of company, type of activity and location. For example, providers who are not headquartered in the UK have, in general, estimated higher costs for the proposed requirements to hold UK-based capabilities to secure and maintain networks.

6.78. For Tier 2 providers, the central estimates for one-off costs as a percentage of turnover were significantly varied across providers, ranging from 1% to 19%. Central estimates

for annual ongoing costs as a percentage of turnover per provider were closer in range from 1% to 7.3%. We believe this variation is explained by the same factors affecting Tier 1 providers. The other key differentiator is whether or not they own and operate their own network. We have accounted for this variation in our analysis, using providers with code powers[66] (which gives them the ability to build telecoms infrastructure on public land) as a proxy for those who own their own network infrastructure. In our cost models for providers in Tiers 2 and 3, we have assumed that providers without code powers will incur 25% of the costs incurred by providers with code powers.

**Types of costs**

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

6.80. The Electronic Communications (Security Measurements) Regulations have been developed from detailed security analysis conducted by the NCSC that used a threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[67]. The regulations aim to address the security risks facing networks and service providers. In fact, our survey found that providers already considered that they met a large number of the requirements. When asked:

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

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

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

6.82. Reflecting the range of providers affected, the key cost drivers cannot be neatly summarised. On average, we found that Section 3 Network architecture, Section 4 Protection of data and network functions and Section 6 Monitoring and analysis had the highest central one off costs and ongoing costs. These costs are likely driven by the breadth of these regulations but we also note that many providers are affected by the

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

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

need to apply the regulations to legacy equipment, requirements around customer premises equipment, the storage of data and data localisation.

6.83. The impact of the regulations and code of practice on legacy systems was an area of focus for the consultation preceding this impact assessment. The responses to the consultation implied that large one-off costs will be needed to remove hardware and legacy equipment which will involve updating infrastructure. Telecoms providers were unable to provide precise cost estimates for these examples.

6.84. Tables 6 and 7 give a breakdown of the costs incurred per Regulation, based on the survey responses.

**Table 6: One-off implementation costs split by Regulation for Tier 1 and 2**

| | | % of total one-off cost |
|---|---|---|
| **Section of the Regulations** | | **central** |
| Network architecture (section three) | *One off costs (£m)* | 24.53% |
| Protection of data and network functions (section four) | *One off costs (£m)* | 21.36% |
| Protection of certain tools enabling monitoring or analysis (section five) | *One off costs (£m)* | 8.62% |
| Monitoring and analysis (section six) | *One off costs (£m)* | 12.87% |
| Supply chain (section seven) | *One off costs (£m)* | 6.20% |
| Prevention of unauthorised access or interference (section eight) | *One off costs (£m)* | 7.76% |
| Remediation and recovery (section nine) | *One off costs (£m)* | 5.15% |
| Governance (section 10) | *One off costs (£m)* | 2.26% |
| Reviews (section 11) | *One off costs (£m)* | 1.90% |
| Patches and updates (section 12) | *One off costs (£m)* | 4.69% |
| Competency (section 13) | *One off costs (£m)* | 1.28% |
| Testing (section 14) | *One off costs (£m)* | 1.45% |
| Assistance (section 15) | *One off costs (£m)* | 1.96% |

**Table 7: Annual ongoing costs split by Regulation for Tier 1 and 2**

| Section of the Regulations | | % of total ongoing costs central |
|---|---|---|
| Network architecture (section three) | *Ongoing costs (£m)* | 14.03% |
| Protection of data and network functions (section four) | *Ongoing costs (£m)* | 17.34% |
| Protection of certain tools enabling monitoring or analysis (section five) | *Ongoing costs (£m)* | 6.62% |
| Monitoring and analysis (section six) | *Ongoing costs (£m)* | 13.81% |
| Supply chain (section seven) | *Ongoing costs (£m)* | 6.16% |
| Prevention of unauthorised access or interference (section eight) | *Ongoing costs (£m)* | 10.06% |
| Remediation and recovery (section nine) | *Ongoing costs (£m)* | 5.84% |
| Governance (section 10) | *Ongoing costs (£m)* | 4.99% |
| Reviews (section 11) | *Ongoing costs (£m)* | 3.58% |
| Patches and updates (section 12) | *Ongoing costs (£m)* | 8.30% |
| Competency (section 13) | *Ongoing costs (£m)* | 2.90% |
| Testing (section 14) | *Ongoing costs (£m)* | 4.26% |
| Assistance (section 15) | *Ongoing costs (£m)* | 2.10% |

6.85. It was also evident that respondents' estimates were subject to some uncertainty. In follow up interviews, respondents noted there were some unknowns that could impact their cost estimates; including the impact of passing requirements onto suppliers; uncertainty around legacy systems and security hardening of end user devices.

### Costs incurred by Tier 3 providers

6.86. This section, sets out evidence gathered regarding the costs imposed on small providers (those that we expect to fall into Tier 3) as a result of complying with the regulations.

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

6.88. We issued the industry cost survey in March 2022 through ISPA, the UK's trade body for internet service providers[68], and FCS, an industry association for communications services providers and sent the survey directly to over 250 telecoms providers. The cost impact survey issued by DCMS received a low response rate (1%) from providers who are expected to fall into Tier 3. In an attempt to increase the number of responses, we extended the survey deadline by an additional two weeks to 26 April and asked FCS and ISPA to specifically encourage those members that we expected to fall into the Tier 3 population to complete the survey. We also disseminated the survey through TechUK, the UK's technology trade association. Despite these efforts, we still only received a total response rate of approximately 1% of the Tier 3 population..

6.89. As with Tiers 1 and 2, we consider the range of cost estimates given in the survey. For Tier 3 providers with code powers, central estimates for one-off implementation costs ranged from £1m to £25m in the survey responses. The central estimates for annual ongoing costs ranged from £100,000 to £2m for Tier 3 providers without code powers.

6.90. These costs are much higher in relation to turnover than costs reported by Tier 1 and Tier 2 operators. This difference may have been affected by the survey design. The cost ranges offered in the survey were very large relative to the turnover of many Tier 3 providers, leading to a large range for costs as a percentage of turnover. In addition some Tier 3 providers did not complete the cost survey in its entirety. We were also unable to gain additional data on specific cost estimates attributed to parts of the regulations as well as relevant turnover for one provider via the cost survey, clarification interviews and email correspondence thereafter. As a result, we have had to make assumptions regarding omitted cost data and relevant turnover by taking averages across medium and large Tier 3 providers with code powers.

6.91. As well as the reasons detailed for Tier 1 providers, we consider the variation across Tier 3 providers cost estimates can be explained by the significant variation in the size of provider. Tier 3 survey respondents revenue varied significantly with one provider not holding code powers.

**Costs incurred by Tier 3 providers with code powers**

6.92. In order to consider the potential scale of the impact on Tier 3 providers, we have used the survey data to produce a range of costs estimates for Tier 3 providers with code powers. It is important to note that this is based on a small sample size and we are not confident that these estimates are an accurate representation of the true costs incurred.

6.93. We split respondents by size and used survey responses to identify the mean low cost estimate and the mean high cost estimate for each size category. The survey asked respondents to select a cost range; the lower bound informs our low estimate and the

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

higher bound informs our high estimate. The central estimate is the midpoint between the low and high estimates for each respondent due to lack of further qualitative data available to us.

6.94. We consider there is likely to be significant selection bias in the responses from Tier 3 providers. We expect that the Tier 3 providers who responded to our survey are likely to be the providers who will be most affected and thus will incur the highest costs. Providers with the greater capacity to respond to our survey are likely to be the Tier 3 firms whose activities are most impacted, and thus incur greater adherence costs to the regulations. This suggests an upward bias in our Tier 3 survey results.

6.95. To account for this selection bias, we have assumed that the 3 Tier 3 respondents (with code powers) are in the upper quartile of businesses in terms of cost impact. There are approximately 90 Tier 3 providers with code powers. Assuming that the 3 providers who responded to the survey are in the top 25 percentile of Tier 3 providers in terms of cost impact. This is equivalent to applying a discount factor of 0.6 to the mean costs provided in the survey responses[69]. We consider this discount would address any selection bias that is present in the cost estimates given in the survey.

6.96. This approach produces the total cost estimates for Tier 3 providers with code powers shown in table 8 below.

Table 8: Total cost estimates for Tier 3 providers with code powers

| | Total costs in net present value terms over the period 2022 - 2031 (3.5% discount rate), £m | | |
|---|---|---|---|
| | Low estimate | Central estimate | High estimate |
| One-off implementation costs | 120 | 370 | 610 |
| Annual ongoing costs | 20 | 30 | 40 |
| **Total costs incurred** | **280** | **670** | **1040** |

**Costs incurred by Tier 3 providers without code powers**

[69] We expect the cost estimate calculated from the survey responses to be the mean cost for the 23 companies who are most impacted by this legislation (upper quartile). We assume that the next 23 companies will incur mean costs of 71% of the upper quartile; the next 23 will incur mean costs of 43% of the upper quartile; and the final 23 companies will incur mean costs of just 14% of the upper quartile. The discount factor of 0.6 is calculated when we take the estimated average costs of all Tier 3 providers with code powers and divide this value by the mean cost of providers in the upper quartile. Further detail on this assumption has been explained in a confidential note to the RPC.

6.97. Since we did not receive any survey responses from Tier 3 providers without code powers (except from one micro-business who are exempt from the legislation), we do not have any evidence on which to base our cost estimate. However, recognising that it is important to include all direct costs to business in our assessment of the business impact, we have included an estimate of the costs incurred by these providers.

6.98. We expect that many of these providers will be largely unaffected as their activities do not align with those targeted by the regulations. However, we do not have enough information on the activities of Tier 3 providers to make an assumption on the number of providers whose activities fall largely outside of the scope of the regulations.

6.99. Instead, we have made an assumption on the costs that will be incurred by Tier 3 providers without code powers as a proportion of those incurred by Tier 3 providers with code powers. For Tier 2 providers, we assumed that all providers without code powers will incur 25% of the costs of those providers with code powers. This was based on last years survey data from Tier 2 providers without code powers and was a conservative assumption[70]. We have assumed that providers without code powers will incur 25% of the costs of those providers with code powers. The resulting estimates are shown in table 9 below. The total estimated cost range for Tier 3 providers without code powers is £200m - £800m between 2022-31[71], in net present value terms.

**Table 9: Total cost estimates for Tier 3 providers without code powers**

| | Total costs in net present value terms over the period 2022 - 2031 (3.5% discount rate), £m | | |
|---|---|---|---|
| | Low estimate | Central estimate | High estimate |
| One-off implementation costs | 90 | 270 | 450 |
| Annual ongoing costs | 10 | 20 | 30 |
| **Total costs incurred** | **200** | **500** | **800** |

6.100. We consider the assumption that providers without code powers incur 25% of costs incurred by providers with code powers to be an overestimation. As noted, we do not have a clear picture of the activities undertaken by Tier 3 providers without code powers and it is likely that many do not undertake a high proportion of regulated activities and thus will not be required to comply strictly with the regulations and thus will incur lower

[70] 25% was a conservative figure chosen as our best guess for the proportion of costs incurred by providers without code powers compared to those with code powers. Further information has been provided to the RPC in a confidential note.

[71] These cost estimates are 25% of the average estimated cost per provider for Tier 3 providers with code powers.

costs. Recognising that it is important to include all direct costs to business in our assessment of the business impact, we have included these costs in our final calculations.

6.101. If we were to assume that providers without code powers incurred 10% of the costs of firms with code powers, this cost range would fall to £80m - £300m. As highlighted above, micro businesses are exempt from the legislation, so we have assumed micro businesses will incur no costs.

6.102. Our total cost estimates for all Tier 3 providers is of a similar magnitude to the total Tier 3 costs estimated in last year's assessment of the draft regulations and draft code of practice. This supports our view that Tier 3 providers will not be disproportionately impacted by the final regulations and code of practice as our Tier 1 and Tier 2 total cost estimates are also of similar size to last year's equivalent assessment. These results highlight that Tier 1 and 2 providers will bear the majority of the costs from the regulations and also imply that our approach to estimating Tier 3 costs is consistent and representative.

**Supplementary Options Analysis: One-off and Ongoing costs**

6.103. This supplementary options analysis considers the impact of Options 1 and 2 on the one-off and ongoing costs that will be incurred by firms implementing the new security framework.

6.104. We consider the following potential impacts of options 1 and 2:

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

6.105. In our consultation stage impact assessment, we considered it likely that the costs of option 1 (the preferred option) will be lower in comparison to option 2. In this impact assessment we have estimated that this indeed will be the case. The degree to which this is the case in reality will depend on the incremental costs incurred by providers when implementing change more quickly and the degree to which the longer implementation timetables in option 1 allow smaller providers to replace legacy equipment before requirements are applied to it. During the consultation on the regulations and code of practice as well as follow-up meetings with telecoms providers we received consistent feedback that shorter implementation timetables would create costly challenges for providers.

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

6.106. In the survey that we carried out in March 2022, we asked providers 'How do you plan to comply with the draft security requirements to be contained in secondary legislation?', the options were:

- By implementing the requirements set out in the draft code of practice

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

6.107. 80% of respondents said that they plan to implement the requirements set out in the draft code of practice where possible but for 'some' areas they will set out their own approach. The reasons given for this are outlined in Table 10:

**Table 10: how firms will comply with the draft regulations whilst setting out own approach for some areas**

| # | Q2.3b. how do you plan to comply with the draft regulations and what are your reasons for this? | % of respondents |
|---|---|---|
| 1 | Difficult to implement requirements set out in the Code of Practice due to legacy systems | 23% |
| 2 | To be more cost-effective | 20% |
| 3 | To maximise network security | 31% |
| 4 | To align with our company's global approach | 14% |
| 5 | We prefer another approach, please explain | 11% |

6.108. The responses suggested providers expect to have lower costs by not complying with the Code in some areas. For instance, under the third option, the code of practice would be implemented with no further regulations set out in secondary legislation. This option could change the way in which the code or practice is implemented.

6.109. We also note that, at the time the survey was carried out, the draft code of practice was published and respondents were advised to use these resources. Therefore, respondents were able to consider the impact from the published code of practice. Whereas, last year, respondents were asked to use a proxy as it had not been published at the time.

**Direct Impact of Implementation Timetables**

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

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

6.112. For the smallest providers in Tier 3, we note that while Ofcom will focus on oversight of Tier 1 and Tier 2 providers, Tier 3 providers may choose to adopt the measures

included within the draft code of practice where these are relevant to their networks and services.

6.113. Options 1 and 2 therefore have the potential to lead to different overall costs as we have demonstrated in our Full Economic Assessment. First, this is because over the 10 year assessment period the costs of option 1 will be lower if Tier 2 providers begin complying with the regulations later. Our central estimate under option 1 gives a total cost incurred by Tier 1 and 2 providers of £3.5bn over the next ten years in net present value terms. This is based on Tier 1 providers incurring one off costs over the years 2022 to 2027 and ongoing costs from October 2022 onwards. We assume that Tier 2 providers will spread one-off costs from 2023 to 2027 and incur ongoing costs from 2023 onwards. If Tier 2 providers began incurring both implementation and ongoing at the same time as Tier 1 our central estimate would increase to £3.6bn.

6.114. Second, costs may vary if the implementation timetable guidelines impact costs for providers. There are a number of potential areas of incremental costs for smaller providers under option 2, as faster implementation might:

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

6.115. Whilst, these impacts might affect any provider they may affect smaller providers proportionately more if they have less capacity for organisational change. During the formal consultation DCMS received further qualitative evidence on the potential impacts option 2 (implementation plus) may have on providers. This includes:

- giving smaller providers limited time to put in place the arrangements required to secure compliance with security provisions which may inadvertently prolong the existence of less secure small network providers
- easing the pressure on Tier 1 providers who may have otherwise had to insource or increase trade amongst themselves. This may result from Tier 2 and Tier 3 providers being reluctant to engage in certain activities with the largest providers as they may be required to comply with the earlier Tier 1 implementation timescales. This could narrow the market for all providers

6.116. We have provided a quantitative assessment of option 2, after reissuing our cost survey, for this impact assessment. The summary analysis and evidence for option 2 can be found in the Full Economic Assessment.

**Impact of Implementation Timetables on legacy equipment**

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

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

6.119. The implementation timetables set out in options 1 and 2 seek to take into account existing public commitments to phasing out legacy systems. This includes the alignment of significant technical changes that would affect fixed networks with the 2025 switch-off date for PSTN and transition to Voice-over-IP (VoIP) networks.

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

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

6.121. Despite these mitigations some providers will incur costs securing equipment and systems considered 'legacy'.

**Compliance and reporting costs incurred by industry**

6.122. The Act gives Ofcom a new general duty which seeks to ensure public telecoms providers comply with their telecoms security duties. This gives Ofcom a clear remit to work with telecom providers to improve their security and monitor compliance.

6.123. To allow Ofcom to fulfil this role, the Act provides Ofcom with powers to monitor and enforce industry compliance with the duties and requirements. It places expanded obligations on public telecoms providers to share information with Ofcom that is necessary to assess the security of their networks. Ofcom will also have the power to ensure public telecoms providers complete system tests, to make staff available for interviews and finally the authority that grants Ofcom providers' the right to a premises in order to inspect, equipment and observe tests. Ofcom will take any relevant provision of the codes of practice into account when carrying out its role.

6.124. In cases of non-compliance, Ofcom will be able to issue a notification of contravention to public telecoms providers setting out the suspected non-compliance, which should include details of any financial penalties that Ofcom is intending on imposing, along with any remedial actions that Ofcom thinks it should e take. Ofcom is then able to confirm the imposition of said financial penalties or remedial actions through a confirmation decision, should it consider it appropriate to do so. The Act also provides Ofcom with a new power that instructs public telecom providers to take the necessary interim steps to address security gaps during the enforcement process.

6.125. Ofcom is required to prepare and publish a statement of their general policy with respect to exercise of their functions by virtue of section 105Y of the Act. This statement will contain Ofcom's final reporting framework and is due to be published in advance of commencement of the new framework in October 2022. The costs to industry of this framework will depend on the frequency and style of compliance reporting required.

6.126. For the purpose of this impact assessment, we made the assumption that the reporting framework set out by Ofcom will require providers in Tier 1 and 2 to produce annual

reporting statements against compliance with the legislation. Ofcom may also issue assessment notices to providers which are likely to be information gathering exercises. These costs will be incurred directly by telecoms providers.

6.127. Deloitte produced a report in 2006 on the regulatory costs incurred by financial services firms in complying with specific FCA regulations[72]. The report considered incremental regulatory costs (costs that would not be incurred if the regulation did not exist) as a % of the total operating cost of each firm. In general, none of the requirements related to periodic reporting attracted high incremental regulatory costs. Although some of these activities are considered to be highly incremental in nature (i.e. the activities would largely not be undertaken in the absence of the FSA requirement), they are not deemed to be costly activities.

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

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

6.130. Due to the large variation of operating costs across Tier 1 and Tier 2 providers, a median annual operating cost figure of £251.5m has been used[73].

6.131. Based on this, compliance and regulatory costs will be £251,500 per year for Tier 1 and 2 providers. This value is based on the methodology used in the Deloitte report (2006), however a clarification interview with a Tier 1 provider suggests that these costs could be as low as £100,000 per year.

6.132. The total estimated average annual cost of reporting is £6m for Tier 1 and Tier 2 providers in present value terms. We have been unable to estimate split reporting costs for Tier 1 and Tier 2 providers. As a result, we have had to make a simplifying assumption that compliance costs are the same across Tier 1 and Tier 2 providers. We assume that Tier 1 providers start incurring reporting costs one year earlier (2024 - 2031) than Tier 2 providers (2025 - 2031) to reflect the different implementation timeframe outlined in our preferred option.

6.133. The code of practice, as set out in the consultation, proposes a phased approach to implementation. This is due to the variation in complexity and cost of the guidance as well as the different points providers will be starting from in regards to implementing the changes. Our modelling approach to compliance and reporting costs reflect the agreed implementation timeframes below:

- **31 March 2024 (Tier 1 only)** - completion of the lowest complexity and least resource-intensive actions

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

[73] The annual operating cost estimates for Tier 1 and Tier 2 providers were sourced from the FAME company database.

- **31 March 2025** - completion of the remaining low complexity actions achievable with minimal resource allocations for Tier 1; and both the lowest complexity and least resource-intensive ow complexity actions for Tier 2
- **31 March 2027** - completion of actions which require devotion of new resources and a degree of complexity (Tier 1 and Tier 2)
- **31 March 2028** - completion of high complexity and resource-intensive actions that must take account of wider change programmes or require deeper, strategic solutions (Tier 1 and Tier 2)

**Monitoring costs**

6.134. Monitoring costs are costs incurred by Ofcom and DCMS in relation to the duties and powers set out in the Telecommunications (Security) Act. These costs are incurred directly by government (DCMS costs) and funded by government[74] (Ofcom costs). As a result, we do not include these costs as a direct cost to business because the impacts do not fall on those businesses subject to the Regulation and accountable for compliance.

6.135. Costs recovered by Ofcom directly from business - i.e. any costs relating to assessment and inspection notices - are discussed separately in the section on Compliance and reporting costs incurred by industry.

6.136. Ofcom already has responsibility for oversight of provisions of the CA which require network providers and service providers to ensure security and integrity of public electronic networks and services. As part of this responsibility Ofcom has published guidance, which was updated in 2017[75].

6.137. Ofcom's role also includes following up and investigating reported incidents and any other concerns when needed and publishing a summary of incidents. As a result of the Telecommunications (Security) Act, Ofcom will be given an expanded duty to seek to ensure industry compliance with new security duties, taking regard to the ode of practice in their regulatory work.

6.138. The Department for Digital, Culture, Media & Sport (DCMS) will also incur additional costs in providing administrative support for the SoS under the new security regime. It is expected that both Ofcom and DCMS will incur costs in carrying out these functions for the new security framework. We estimate these costs in Table 8 below based on information provided by both Ofcom and DCMS in April 2021.

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

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

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

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

applied.[76] Ofcom cost estimates are unlikely to change significantly with the implementation of our preferred option 1 or option 2 (Implementation plus), with the latter option not granting a grace period for Tier 2 providers.

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

6.142. DCMS costs are a best estimate of future resource requirements so we have indicated a range of costs, using a 25% discount on the base estimates to find the low estimate and a 25% load to find the high estimate. These costs relate to the regulations; other costs will be incurred with respect to the national security powers in relation to high risk vendors:

**Table 11: Costs of monitoring compliance with Part 1 of the Telecommunications (Security) Act**

| | Total costs in net present value terms over the period (3.5% discount rate), £m | |
|---|---|---|
| | Low estimate | High estimate |
| Ofcom costs | 53.4 | 70.4 |
| DCMS costs | 0.9 | 1.4 |
| Total | 54.3 | 71.8 |

**Indirect costs: Impact on the supply chain**

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

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

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

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

6.146. We estimate that there were at least[77] 104[78] suppliers in the UK's telecommunications sector from 2017 to 2021, based on publicly announced carrier-vendor contracts. This is in contrast to 746 suppliers who operated globally over the same time period.

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

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

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

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

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

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

**Indirect costs: impact on consumers**

6.152. We also consider that end users of telecoms networks and services may potentially incur costs as a result of telecoms providers passing the costs of compliance onto consumers. The extent to which changes in network costs are passed through to consumers depends on the level of cost reduction as a proportion of total cost and the rate of cost pass-through. A 2009 report by the International Telecommunications Union (ITU) found that the pass-through rate of costs to consumer prices was 69% in the mobile telecoms market and 26% in the fixed telecoms market.[79] Costs that are not passed through to consumers and business customers are either retained by telecommunications providers or are passed through to network investment

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

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

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

expenditure. This means that in addition to the pass-through of costs to consumers, costs incurred by telecoms providers could also lead to less investment in networks.

6.153. In follow-up clarification meetings with providers, the general consensus was that implementation of the regulations and code of practice would inevitably lead to increased costs passed onto business customers and consumers. One provider highlighted that this was particularly challenging for them as it is 'difficult to sell this type of cost to consumers as they do not really value telecoms security and resilience'. Another provider shared that it is currently not possible to quantify what increased costs might be for consumers but it may be a holistic industry approach once the costs of the new security framework are better understood. One provider provided a contrasting opinion however, stating that the new regulations and code of practice would not necessarily mean higher costs for consumers. This provider highlighted that there were many other factors beyond security and resilience (such as macroeconomic considerations) which would have a greater impact on consumer prices.

6.154. Our analysis shows that the new security framework will lead to material costs for telecommunications providers in the UK. Since we have only quantified the total costs incurred by telecom providers in this impact assessment, and not the total benefits, we do not have an estimate for the total net costs incurred by telecoms providers.

## Economic Impact - benefits

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

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

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

6.158. Table 12 sets out the potential benefits of the regulations identified by providers in our cost impact survey, which received 15 responses.

**Table 12: What benefits do you expect will accrue to your business from implementation of the draft Electronic Communications (Security Measures) Regulations 2022? All responses[80].**

| Answers | Percentage of respondents that selected this benefit |
|---|---|

[80] Note: All responses have been provided. Respondents were asked to tick all that apply.

| | |
|---|---|
| Detect security compromises earlier | 19% |
| Reduce number of security compromises | 14% |
| Reduce severity of security compromises | 14% |
| Improve ability to rectify security compromises | 14% |
| Reduce number of network outages | 8% |
| Reduce severity of network outages | 8% |
| Improve ability to rectify network outages | 8% |
| Improve offering to customers | 8% |
| No real benefit | 6% |
| Other, please specify | 0% |

6.159. Approximately 60% of respondents that completed the cost impact survey expect the benefits from implementation of the regulation and code of practice will help to improve the prevention and handling of security compromises whereas 24% expect it to improve network outage related issues.

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

6.161. We also consider the economic benefit arising from 5G use cases, where network security and resilience are considered a prerequisite to their adoption. These are a key indirect[81] benefit resulting from the new security framework.

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

**Evidence of current vulnerabilities in the network**

6.163. As wider UK Critical National Infrastructure becomes more dependent on the UK's telecoms networks with the roll-out of full-fibre and 5G, it is vital that security concerns are properly accounted for and addressed. There is clear evidence of the telecoms sector's increasing vulnerability to security incidents prior to the pandemic.

6.164. 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 (CSP)[82]. The 2021 Nextguard's DDoS Threat report measures the trend in which attackers launched DDoS attacks at single targets within a CSP, with an attack size increase of over 500% quarter 2 to quarter 3 and over 200% 2020 to 2021[83].

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

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

[83] https://blog.nexusguard.com/threat-report/ddos-threat-report-q3-2021

EfficientIP's 2017 Global DNS Threat Survey Report, which surveyed 1,000 global telecoms providers and vendors, states that 25% admitted they have lost sensitive customer information as a result of a DNS attack[84]. This is higher than any other sector surveyed.

6.165. As well as security attacks, telecoms networks are vulnerable to outages which have an impact on all users of networks. In 2019, of the 61 serious or severe outages that made headlines globally, 30% were caused by network issues, according to a 2020 Uptime Institute Report[85]. This was the second biggest cause of outages, narrowly surpassed by IT system issues at 31%.

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

- Within the last five years, a major telecoms network was accidentally remotely disabled for a number of hours due to the failure of a critical core node to process an unusual, internationally-routed signalling message. While this failure was an accident, it highlights a potential vulnerability that could be intentionally abused unless mitigated. Furthermore, signalling networks have been shown to allow the leaking of subscriber and network data, sometimes in support of criminal activity.
- On 20 December 2018, HMG attributed a cyber attack targeting several global managed service providers (MSPs) to China-linked group APT10. Through compromise of these MSPs, APT10 had managed to exploit multiple customers of those MSPs and exfiltrate a high volume of data. The overall scale of the compromise was unprecedented, and had gone undetected since at least 2016. Other recent case studies of security incidents in the UK include the below:
- O2 suffered a major network failure in December 2018 due to an expired certificate in Ericsson software, which resulted in a loss of data services. 32.1m users in the UK had their data network go down for up to 21 hours. Other services which rely on O2's network, such as TfL's live bus timetable and all the apps that make calls to the API also went down.[86]
- 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.[87]
- In March 2015, internet traffic for 167 BT customers, including a UK defence 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.[88]
- According to the NCSC, one company affected by the so-called NotPetya attack in June 2017 had to install 4,000 new servers, 45,000 new PCs and 2,500 new applications.[89]

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

[85] Uptime institute: Annual outage analysis, 2020

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

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

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

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

- In 2016, UK mobile provider Three was hacked, resulting in the theft of personal data from 134,000 customers. The hackers accessed information using employee login details.[90]
- In 2016 it was reported that malicious software known as the 'Mirai Worm' had infected around 100,000 Post Office routers in the UK. The hacked routers were used to route internet traffic to popular websites including Netflix and Twitter.[91] An independent testing body suggested that this could have arisen from a weakness in some of the routers' software.[92]

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

6.168. According to a 2020 study by IBM, a majority of organisations (54%) required remote work at the height of the COVID-19 pandemic[93]. This is compared to 5% of workers working from home all the time in January to March 2020, according to a survey undertaken by the Chartered Institute of Personnel and Development (CIPD)[94]. This trend in remote working makes it more vital than ever to ensure households and businesses are kept online with as few disruptions as possible.

6.169. 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 Cyber Security Breaches Survey, undertaken by Ipsos Mori and published by DCMS in March 2020[95]. The information and communications sector has, across each year of the survey, consistently stood out as more likely to identify breaches. 62% of information and communications companies have identified breaches or attacks in the last 12 months, compared to 46% across all UK sectors and 47% for the same sector last year. A report from OGL Computers found that 75% of SME IT and telecoms companies in the UK suffered 2 or more cyber attacks in 2020[96].

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

### Costs of security incidents

6.171. There are a range of costs identified across literature and case studies, however, the general consensus is that these costs are significant.

6.172. The Cyber Security Breaches Survey 2022[97] states that the average cost of all the cyber security breaches experienced across all sectors in the past 12 months is

---

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

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

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

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

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

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

[96] OGL, State of Technology Research Report

[97] Cyber Security Breaches Survey 2022

estimated to be £4,200. For medium and large firms, the average cost is higher at £19,400.

6.173. The findings from last year's Cyber Breaches Survey 2021 have been extrapolated to provide a cost estimate across all UK businesses for that year. The estimated cost to UK businesses of cyber breaches is £648 million in the central scenario, within a range of £356 million to £939 million (with a 95% confidence interval). It is important to note that survey respondents were asked to identify impacts from the breaches or attacks.[98]. There is an acknowledgment of the lack of a framework to measure the financial impacts of cyber attacks. This can lead to underreporting as well as some organisations having a reduced ability to identify the types of costs associated from those attacks. Additional DCMS research[99] has shown that respondents do not fully count all economic costs, instead focusing on direct financial impacts. As such, the figures are more often than not an underestimate.

6.174. The IBM 2020 Cost of Data Breach Report found that the average total cost for UK data breaches between August 2019 and April 2020 was $3.90 million.[100] An EfficientIP report found that, specifically for the telecoms sector, the average cost of a single cyber attack was $600,000 in 2017 (global figure)[101]. Furthermore, 5% of telecoms organisations surveyed stated an attack cost them more than £3.75 million. According to a Accenture report, the average annual cost of cybercrime for a company with over 5,000 employees was $11.5m in 2017[102].

6.175. Of the case studies discussed above, only the TalkTalk and NotPetya incidents have made the costs publicly available. The total cost to TalkTalk was £60m and the cost to the company affected by the NotPetya attack was estimated at £150 to £250 million[103].

6.176. In many cases, a security compromise also has a reputational impact on the affected company. According to a CGI and Oxford Economics report, an organisation's share price falls by an average of 1.8% following a severe breach. This is equivalent to a £120m loss of FTSE 100 company value following a severe cyber breach. In extreme cases, cyber breaches have reduced a company's share price by 15%[104].

6.177. All of the estimates given here suggest that the cost of a security breach or attack for a UK telecoms company could be anywhere between £4,000 to £250m. For the purpose of this impact assessment, we have made some key assumptions to illustrate the potential benefits associated with the improved security of telecoms networks. We have used the EfficientIP and Accenture cost figures, as well as the CGI share price impacts,

---

[98] Survey respondents were asked to identify breaches or attacks: new measures needed for future attacks, added staff time to deal with breach or inform others, stopped staff carrying out daily work, other repair or recovery costs, prevented provision of goods and services, loss of revenue or share value, complaints from customers, reputational damage, discouraged you from carrying out a future business activity, goodwill compensation or discounts given to customers and fines or legal costs.

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

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

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

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

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

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

to estimate the total cost of security compromises affecting providers of PECN and PECS in the UK over the next ten years.

6.178. We have assumed that for Tier 1 and 2 providers, the current annual cost of cyber security compromises is equivalent to £9.0m per company, as set out in the Accenture report. We have also assumed that, over the next ten years, there will be two severe incidents which reduce the share price of the affected provider, resulting in a loss of £120m per incident. This is based on the occurrence of two severe cyber compromises affecting major telecoms companies in the UK between the years 2011-20[105].

6.179. For Tier 3 providers we decided to take a more conservative approach to calculating the costs of security compromises. This is because the cost estimates highlighted above from security breaches are likely to be an overestimate for those providers that fall into the Tier 3 category. From our literature review we did not find appropriate security compromise estimates for smaller telecoms providers. As a result we have taken an average of the monetisable costs of security compromises as a percentage of our central total estimates for Tier 1 and Tier 2 costs from the regulations. We have then applied this percentage estimate, of security compromises as a proportion of total costs by tier, to our total Tier 3 central cost estimates[106].

6.180. Table 13 shows the total cost of security compromises for PECN and PECS providers over the years 2024 - 2031. This period starts in 2024, two years after the measures in the code of practice have commenced, giving time for them to begin to impact the costs of security compromises. This will continue to the end of the impact assessment period.

**Table 13: Monetisable costs of security compromises for PECN and PECS providers, discounted at 3.5% over 2024-31**

| | Total cost (£bn) |
|---|---|
| Tier 1 providers | 0.42 |
| Tier 2 providers | 1.40 |
| Tier 3 providers | 1.28 |
| Share price impact | 0.20 |

6.181. The total security compromises cost over the impact assessment period for PECN and PECS providers is estimated to be £3.3bn.

6.182. We have conducted some sensitivity analysis on these assumptions. In the low cost scenario, we assume that Tier 2 providers incur a lower average annual cost per breach which is equivalent to £474,000 based on the EfficientIP report and that there will only be one severe security compromise impacting the share price of a Tier 1 provider. In this case, the total cost of security compromises over the period is £2.0bn. In the high cost scenario, we assume the same as our central scenario but there will be three severe security compromises impacting the share price of a Tier 1 provider as opposed

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

[106] Due to unsuitable cost estimates of security compromises for Tier 3 providers we have taken an average of security compromise costs by tier as a percentage of total (one-off and ongoing) costs for Tier 1 providers (15%) and Tier 2 providers (202%). We have then applied this average percentage estimate to our central Tier 3 total costs from the regulations and code of practice.

to two. In this case, the total cost of security compromises over the period is £3.9bn. Due to a lack of evidence on the cost of security compromises for smaller telecoms providers we have taken the conservative approach which assumes Tier 3 costs in the low and high cost scenarios are the same as in our central scenario.

6.183. The new security framework introduced by the Act will reduce the cost impact of security compromises in two ways. Firstly, any security compromises that do occur are likely to be identified and dealt with at an earlier stage due to the monitoring and analysis requirements in the regulations. Providers are required to monitor incoming and outgoing communications to identify and investigate anomalous activity. The remediation and recovery requirements in the regulations are aimed at making sure networks can be recovered after any security compromises. In the UK, it takes an average of 181 days to identify a data breach and 75 days to contain it[107]. The average cost savings of containing a breach in less than 200 days, compared to more than 200 days is $1.12 million[108], representing a 26% reduction in the average cost of a breach.

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

- Regulation 3 - Network architecture: This includes keeping the most sensitive parts of their network separate to the less sensitive parts.
- Regulation 8 - Prevention of unauthorised access or interference: This Regulation contains measures to protect networks by controlling who has permission to access network functions. This includes using best practice technical solutions like multi-factor authentication and limiting the number of people given security permissions. It also requires providers to be able to isolate parts of the network that are essential for it to run from any unsafe signals that come from outside the network.
- Regulation 10 - Governance: amongst other things, providers must also identify and prioritise necessary network security updates and network equipment upgrades.
- Regulation 14 - Testing: This Regulation ensures that providers must carry out or arrange tests on their network or service to assess the resilience of the network or service to security risks. These tests should simulate, as far as is possible, active techniques and realistic situations that might be expected to be used by an attacker.

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

**Benefits to consumers of improved telecommunications security**

6.186. In the above section, we have monetised the potential benefits to telecoms providers of improved security. Improved security will also benefit telecom consumers by ensuring access to the internet and by ensuring private data is not leaked. As of 2021[109], there were 85 million active mobile subscriptions and 27.7 million fixed broadband connections in the UK. A reduction in the frequency and severity of security

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

[108] Comparing the Cost of a Ransomware Attack, 2021.

[109] Telecommunications Market Data Update Q4 2021

compromises in telecoms networks and services will impact consumers in a number of ways. For example, reductions in network outages will enable more continuous access to phone and internet services for consumers. The O2 outage in 2018 left 32.1 million customers without access to the internet, interrupting both business and personal activities being undertaken over the mobile data network. Studies have shown that consumers value network access and resilience. A study by Rand Europe (2014)[110], for example, found that residents in UK not-spot areas are willing to pay up to £23 more a month for better quality service.[111] Separately, a study by Lee and Cho (2018) found that mobile users in South Korea were willing to pay on average $0.80 to avoid communication failures.

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

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

Conclusion: As stated above it is clear to see there are significant financial impacts caused by a lack of telecom security. However, it is difficult to monetise the benefits attached to telecom security due to a lack of available evidence, a lack of robust assumptions in the literature and the potential risk of double-counting.

**Economic benefits of 5G and Full Fibre**

6.189. The uptake and adoption of 5G and full fibre networks in the UK is strongly dependent on a particular level of security and resilience within these networks. The Review states that 'the potential economic and social benefits of 5G and full fibre digital connectivity can only be realised if we have confidence in the security and resilience of the underpinning infrastructure. The widespread deployment of 5G and full fibre networks is a primary objective of government policy. These networks will be the enabling infrastructure that drives future economic growth. The security of these networks is in the UK's economic interest. We define security as safeguarding the availability, integrity and confidentiality of the UK's telecoms networks. If these networks are judged to be insecure, their usage and economic value will be significantly reduced.'[112]

6.190. These communications services have never been more important than in the last year. The Covid-19 pandemic has highlighted the importance of connectivity for UK consumers as it drives how businesses and people communicate and both consume information and entertainment. The steps taken by the UK and devolved governments in response to Covid-19 meant that, during 2020, people relied even more than before on fast, reliable broadband connections in their homes. The UK's fixed access networks have seen significantly increased demand from users in 2020 when compared to

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

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

[112] UK Telecoms Supply Chain Review Report, 2019

periods prior to lockdown, mobile voice traffic increased by 10-45% across the providers[113].

6.191. This dependence on secure and reliable telecommunications networks is expected to continue into the future. A survey completed by just under 1,000 firms conducted in September 2020 by the Institute of Directors (IoD) showed that 74% of firms plan on maintaining the increase in home working[114].

6.192. Several recent reports have estimated the economic benefits of 5G and full fibre-to-the-premises broadband (FTTP) networks to the UK. However, the Covid-19 pandemic and the high risk vendor (HRV) decision made by government in July 2020[115] have impacted the speed at which these networks will rollout. We have considered these impacts in more detail in the next section.

6.193. An independent report from the Centre of Policy Studies finds that, despite the impact of the Covid-19 pandemic, a potential £34.1bn of additional economic output could be created if the government delivers its 5G target of covering the majority of the population between 2021 and 2027, and more than £40bn if this target is exceeded[116].

6.194. As for full fibre, a report from the Centre of Economics & Business Research estimates a gross value added (GVA) uplift of £59 billion by 2025 if deployment is completed at that point – with benefits continuing to rise after deployment is complete. The report forecasts an additional £16.1bn on GVA due to workforce impacts of network deployment[117]. Even with the impacts of Covid-19 and the HRV decision, the government stated in November 2020 that it aims with industry to deliver a "minimum of 85%" gigabit-capable coverage by 2025[118].

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

6.196. The following analysis makes the argument that the economic value generated by a number of 5G use cases are dependent on secure and resilient networks. Without this legislation, the full extent of these benefits will not be realised. In our economic assessment we have not attributed a proportion of these benefits to the new security framework but if a small fraction (e.g. 5%) of the benefits were underpinned by the legislation this would be a significant value.

Conclusion: As noted above there are significant benefits attached to the government's 5G target of covering the majority of the population between 2021 and 2027. These benefits will only be realised if the UK has strong and resilient networks.Therefore, it can be concluded that without the implementation of this legislation the full extent of these benefits will not be realised. The analysis has not aimed to monetise the benefit of a new security framework but even if a small fraction of the benefit was attributed to the legislation this would be significant.

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

---

[113] Connected Nations report 2020, Ofcom

[114] Home-working here to stay, new IoD figures suggest | Institute of Directors | IoD, September 2020

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

[116] Upwardly Mobile: How the UK can gain the full benefits of the 5G revolution, October 2020

[117] Full fibre broadband: A platform for growth, October 2019

[118] National Infrastructure Strategy - GOV.UK, November 2020

6.197. From our literature review of twelve reports[119] published over the last 5 years that have estimated the economic impact of 5G, it is clear that the value of 5G is derived from the potential use cases for businesses and governments. Some examples of these use cases include: smart LED street lighting, which can be dimmed or brightened remotely as needed; 5G sensors on railway lines to improve predictive maintenance; and remote monitoring of soil temperature and moisture, crop development and livestock on farms.

6.198. 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.'*[120]

6.199. The literature shows that some of the use cases rely heavily on networks that are highly secure and reliable. This is backed up by the finding in a 2018 Ericsson report[121] that the two main barriers to 5G adoption are concerns around data security and privacy and lack of standards.

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

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

- Remote medical examination
- Remote health monitoring
- Autonomous cars

6.202. We have estimated the economic value of these cases based on findings in the literature. Table 14 below shows the estimated benefits in the central scenario.

**Table 14 : Monetisable benefits of each 5G use case, discounted at 3.5% over 2022-31**

| Use case | Economic benefit (£bn) |
|---|---|
| Remote medical examination | 6.4 |
| Remote health monitoring | 6.6 |

[119] Research into the economic benefits of 5G is relatively limited so we have taken the twelve reports that we consider to have a robust methodology.

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

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

| | |
|---|---|
| Connected and autonomous cars | 12.5 |
| Total (2022-31) | 25.5 |

6.203. The total monetisable benefits of the three identified use cases over the impact assessment period of2022 to 2031 is estimated to be £25.5bn, in present value terms. However, we note that these benefits are dependent on the roll out of 5G networks and do not begin to accrue until 2026 or 2028 in the case of autonomous cars. The analysis that makes up this figure is detailed in Annex 1.

6.204. We have conducted some sensitivity analysis on these wider benefits to illustrate the impact of varying our assumptions. As a base case, we mapped the estimated benefits to the UK found in the literature for each use case across a ten year period. In the central scenario, shown in Table 16, we have delayed the accrual of benefits by 3 years to reflect the delay in 5G rollout caused by any potential decision to use the HRV powers in the Act [122]. This includes a one year delay as a result of the Covid-19 pandemic, as estimated by a 2020 PwC report[123].

6.205. In the optimistic scenario, we assume that the use of any of the HRV powers in the Act would not delay rollout significantly. In this case, we have assumed a one year delay coming from Covid-19 only. In this case, the total monestiable benefit, discounted at 3.5% over the next 10 years, increases to £44.0bn

6.206. In the worst case scenario, we have assumed a 3 year delay resulting from the HRV decision and Covid impacts, as well as a further two year delay in the deployment of the individual use cases. 5G use cases are still in trial for the most part and we have applied this sensitivity analysis to account for the risks associated with the application of such a nascent technology. In this case, the total monestiable benefit, discounted at 3.5% over the next 10 years, falls to £11.8bn. A delay of two years reflects our estimate of the most likely worst case delay in deployment across the three use cases.

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

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

Conclusion: 5G gives way to a variety of use-cases. The three main use cases as mentioned within Ericsson's report are remote medical examinations, remote health care and finally autonomous cars. In the worst case scenario these use cases deliver an economic benefit of £11.8bn. A secure network is important in helping to deliver these use cases, however there

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

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

are also other important factors that need to be considered. These factors include innovation, skill and access to finance to name a few.

## Costs and benefits to business calculations

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

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

- could incur one-off costs ranging between £1,000m to £2,400m present value terms assuming that these costs are incurred by all providers over the years 2022 - 2027.
- could incur average annual ongoing costs in the range of £100m to £240m per year in present value terms assuming that these costs are incurred by all providers from 2023 onwards (50% in 2023 and 100% thereafter for Tier 2 providers) and from 2022 (at 50% in 2022 and 100% thereafter) for Tier 1 providers.. We estimate familiarisation and compliance and reporting costs for all providers. In total we estimate familiarisation costs will fall in a range from £4.6 - £7.8 million net present value over the impact assessment period; and compliance and reporting costs will be approximately £6 million annually over the same period..

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

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

6.212. 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 regulations. We do not have sufficient information to make this assumption.

**6.213. Instead, we have presented an illustrative breakeven analysis between the direct costs and the potential direct benefits for Tier 1,Tier 2 and Tier 3 providers in Table 16 to assess the magnitude of the policy.**

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

**the central scenario, best-case scenario and worst-case scenario for Direct benefits in Table 15.**

**Table 15: Direct costs and benefits net present value figures over period 2022-31, discounted at 3.5% (Includes one off and ongoing costs for Tier 1, 2 and 3 providers)**

| | Direct costs*[124] (£m) | Direct benefits (£m) | % of direct benefits that need to be realised to break even* |
|---|---|---|---|
| Central scenario | 4,103.9 | 3,302.1 | 124.3% |
| Best-case scenario | 2,233.7 | 3,934.0 | 56.8% |
| Worst-case scenario | 5,800.5 | 1,998.2 | 290.3% |

6.215. This analysis shows that, in the central scenario, over 100% of the estimated direct benefits need to be realised as a result of this legislation in order to cover the costs. This suggests that the direct benefits will not compensate for the direct costs of the new security framework.

6.216. However, it is important to note that our estimated benefits figure uses an average annual cost of cybercrime for enterprises with at least 5,000 enterprise seats[125] as a proxy for the costs of cybercrime to Tier 1 and 2 providers. However, a single incident can have a much more significant impact, for example, the total cost of the TalkTalk case study cited above was £60m and the cost to the company affected by the NotPetya attack was estimated at £150 to £250 million[126]. Furthermore, whilst CGI and Oxford Economics found that an organisation's share price falls by an average of 1.8% following a severe breach, in extreme cases, this impact has been as high as 15%[127].

6.217. As stated, we do not expect that all of these benefits will be realised as a result of the new security framework. These benefits represent the total costs of security compromises to telecoms providers as far as we have been able to monetise them. While we expect that the new framework will reduce the frequency of compromises to a certain extent, we also expect that compromises will still occur but may be identified earlier due to the improving monitoring measures required by the framework. IBM found that identifying and containing a breach early reduces the cost by an average of 26%[128].

6.218. We have not included the wider benefits of 5G use cases that are reliant on highly secure and resilient networks in the above table. We note that the benefits of 5G use cases are indirect and would not be included in the net direct cost to business but in the

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

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

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

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

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

wider net present social value. However, to demonstrate the scale of the wider benefits, we have set them out in table 16 below.

**Table 16: Net present value figures for wider benefits over period 2022-31, discounted at 3.5%**

| £bn | Direct benefits (costs of security compromises) | Indirect benefits (5G use cases) | Total |
|---|---|---|---|
| Central scenario | 3.3 | 25.5 | 28.8 |
| Best-case scenario | 3.9 | 44.0 | 47.9 |
| Worst-case scenario | 2.0 | 11.8 | 13.8 |

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

# 7. Risks and assumptions

7.1. In carrying out this impact assessment we have assessed the direct costs to industry of implementing the regulations based on the draft Electronic Communications (Security Measures) Regulations published on 1 March 2022. The regulations have been developed from detailed security analysis conducted by the NCSC that used a threat model to identify the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[129]. An early draft of the regulations was published in January 2021 to gather industry feedback[130]. The draft regulations published for formal consultation on the 1st March and have since been updated to account for that initial feedback. They aim to address the security risks facing public networks and services providers by providing appropriate and proportionate security requirements in law with which public telecoms providers must comply. Ofcom, as the independent telecoms regulator, will be responsible for monitoring and enforcing compliance with the statutory requirements.

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

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

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

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

**Table 17: Assumptions and their associated risks**

| *Assumption* | *Evidence to support this assumption* | *Risk and mitigations* | *Description of Sensitivity analysis undertaken* |
|---|---|---|---|
| We assume that the regulations and the code of practice continue to create security benefits throughout the impact assessment period. | The regulations are based on a threat model which identified the areas of networks and services most at risk of compromise. A summary of that analysis was published by the NCSC in January 2020[131].<br><br>The final regulations and code of practice will have been updated to account for feedback received in a public consultation. Industry feedback will enable effective targeting of the regulations and code of practice to deliver greatest benefits. | **Medium - Regulations become outdated by technological change.**<br><br>Technology evolves at pace so new individual security controls would be needed if for example, macro shifts (e.g. mass virtualisation, cloud provision of core) lead to a PECN/S focused framework becoming ineffective.<br><br>However, future accompanying codes of practice can be updated periodically, subject to consultation. The legislation may also be amended as necessary following parliamentary procedure.<br><br>Wider DCMS policy planning to address risks of service provision changes and ensure appropriate protections for end-users | The assessment of benefits includes sensitivity analysis to demonstrate the scale of the potential benefits in a low benefit scenario. |
| We assume that PECN and PECS can pass through security requirements to their suppliers through contractual or other means. | DCMS asked questions on supply chain as part of its survey of PECN and PECS. The majority of respondents thought that some or all of their suppliers would be affected and that the regulations would reduce the number of suppliers participating in procurements. | **Low/Medium - PECN and PECS cannot pass on supplier requirements.**<br><br>We consider that this risk is Low to Medium because those vendors that we have engaged with have indicated that they will comply with | Cost assessment is based on PECN and PECS estimates of direct costs that they will incur for each section of the regulations including those on managing the Supply Chain. We estimate an upper and lower bound for all costs impacts We don't estimate wider impacts including the |

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

| | | | |
|---|---|---|---|
| | DCMS also met with a small number of suppliers to discuss the potential cost impact of the regulations.<br><br>This followed a more general round of bilateral engagement with suppliers where DCMS provided a brief history of the rationale behind the security framework and updated on its progress. | the indirect requirements.<br><br>To mitigate this risk DCMS will maintain review of security improvements to gauge effectiveness of the new framework including as part of the Post Implementation Review.<br><br>Furthermore, the wider DCMS programme to diversify the supply chain includes de-risking new entrants via a new UK Telecommunications Lab to enable security research and testing. | impact of a reduction in the number of suppliers in PECN and PECS procurements. We consider the likelihood of significant market exit to be low given the mitigations set out. |
| We assume that Ofcom's monitoring regime provides sufficient oversight and that the penalty regime provides sufficient incentive to comply | We asked PECN and PECS questions on how they would comply with the regulations in our survey. 80% of those that responded said they would comply 'By implementing the requirements set out in the draft code of practice where possible but for some areas we will set out our own approach' The remaining respondents indicated that they would adopt the requirements as set out in the draft code of practice. When asked for the reason for their approach the joint most popular responses were s 'to maximise network security', 'to maximise chances of full compliance' and 'to ensure a standardised approach with other operators'. | **Low - PECN and PECS do not comply with the regulations such that the security outcomes are not achieved.**<br><br>Ofcom is being provided with significant new oversight powers together with a funding uplift to ensure adequate resources and ability to carry out compliance monitoring. Penalty powers in the Act are among the toughest in comparable frameworks and industry and commentators have noted the 'tough' approach being taken. | We assume 100% compliance in the impact assessment. |
| We assume that there will be wider benefits than those monetised in this impact assessment. | The benefits monetised in this impact assessment are only those benefits that we have been able to | **Low - no benefits are accrued other than reduced cost to providers of security** | We have not based any analysis on the assumption that more benefits will accrue than those we have |

| | | | |
|---|---|---|---|
| | estimate. The direct benefits monetised are the benefits of reducing the cost of potential security compromises and the indirect benefits monetised are the benefits of unlocking 5G use cases that are reliant on a secure and reliable network. We assume that there will also be wider benefits that have not been estimated. The new security framework is a regulatory intervention that aims to improve security outcomes for the UK's critical national infrastructure. The wider benefits of improved telecoms security include the benefits to consumers of mitigating the likelihood and severity of network outages and data losses, as well as the prevention of threats to telecoms networks that we are not able to predict or anticipate at this stage.<br><br>For this reason, we assume that the breakeven analysis detailed in section 'Costs and benefits to business calculations' does not fully reflect the proportion of benefits that need to be realised in order to cover costs. | **compromises and the benefit generated by the rollout of specific 5G use cases modelled in the benefits section.**<br><br>The new security framework is designed to improve security outcomes for the UK's telecoms networks and services, which form part of the country's critical national infrastructure. We consider, therefore, that there are more benefits to society than the savings made by telecoms providers in reduced security compromise costs and the value generated by three 5G use cases of remote medical examination, remote healthcare, monitoring and autonomous cars.<br><br>Therefore, the risk that there are no additional benefits on top of those monetised is low. | directly estimated. The breakeven analysis detailed in section 'Costs and benefits to business calculations only uses the direct benefits monetised of reduced cost to providers of security compromises. Based on these benefits only, more than 100% of these benefits need to be realised in order to breakeven against the estimated direct costs. If we include the indirect benefits arising from rollout of 5G use cases that are dependent on highly secure and resilient networks, then 48% of total direct and indirect benefits need to be realised to cover the costs (in a low benefit, high cost scenario).<br><br>Therefore, even if benefits are no higher than those monetised in this impact assessment, total benefits will likely be higher than total costs. |

# 8. Impact on small and micro businesses

### Into what sector and/or subsector the affected businesses fall

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

8.2. Examples of communications providers include[132]:

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

### Number of businesses in scope of the Regulation

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

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

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

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

8.6. We have split these known providers by size according to the number of employees in Table 18, using data on employee numbers from the FAME database, a company information database from Moody's Analytics[133]. Where employee data was not available, we have used total revenue as a proxy measure. This gives an indication of the number of small businesses that are subject to the legislation. However, we note that data on number of employees and revenue is not available for the full dataset. Data is available for 73% of the PECN and PECS providers known to Ofcom; for the remainder we have assumed the same size distribution can be applied. The table shows that there are at least approximately 200 small businesses in our list of PECN and PECS (almost 30%).

**Table 18: Estimate of PECN and PECS split by business size**

| Size | Definition used | Number | % of total number |
|---|---|---|---|
| Large | More than 250 employees (if employee data is unknown, total revenue over £50m) | 105 | 14% |
| Medium | Between 50 and 249 employees, inclusive (if employee data is unknown, total revenue between £10.2m and £50m) | 140 | 19% |
| Small | Between 10 and 49 employees, inclusive (if employee data is unknown, total revenue between £362k and £10.2m) | 207 | 28% |
| Micro | Up to 10 employees (if employee data is unknown, total revenue below £362k) | 302 | 40% |
| Total | | 752 | 100% |

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

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

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

**Type of small and micro businesses that will be affected**

8.9. As set out in our cost benefit analysis, we consider that type of business is likely to be important in determining the costs of implementing the regulations. And that direct

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

costs[134] will be highest for those companies that own and operate their own infrastructure - vertically integrated providers - and the least for resellers who do not own any network infrastructure. Direct costs are more likely to be linked to one off or fixed costs which can have a disproportionate impact on small businesses. Cost analysis based on the cost survey does suggest this could be true as our Tier 3 responses had the highest one-off costs as a % of turnover from implementing the regulations and code of practice. However, because 75% of Tier 3 respondents to the survey held Code Powers and only 1% of the estimated Tier 3 population responded to the survey we cannot confidently extrapolate these findings to all small businesses.

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

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

**Table 19: Breakdown of providers by size and code power status**

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

**Do the impacts fall disproportionately on small and micro businesses?**

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

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

Box 4: Overview of Survey of PECN and PECS

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

To assess the impacts of the regulations we carried out a survey of PECN and PECS.. The survey was sent directly to larger providers with whom DCMS is already engaged on the technical detail of the draft regulations. In order to ensure that smaller businesses replied we also distributed a shorter survey aimed at smaller businesses through the Internet Service Providers' Association (ISPA) and the Federation of Communication Services. To improve the low engagement from smaller providers (observed with last year's survey), DCMS undertook a separate telecoms market research project to better understand the demographics of the telecommunications sector. The project resulted in over 250 contact details of telecoms providers (predominantly smaller providers) who agreed to being recontacted and thus received a direct link to this year's cost survey. Before the survey was issued, DCMS engaged with multiple trade bodies who were representing a wide range of smaller businesses. This engagement was focussed on the recently published draft SI, seeking views on the technical detail of the draft regulations and identifying where concerns existed.

The survey was completed by 3 small and 1 micro businesses. Given that micro businesses are exempted from the Regulation, we note that this is a small sample of the number of smaller businesses likely to be in the scope of the Regulation.

Further to the survey, we also attempted to carry out bilateral clarification interviews with 1 small business, however we were unsuccessful in our attempt to arrange a meeting. .

8.14. Due to the small sample size of the survey, we are not able to split out the data for small and micro businesses. It is important to note that there is no expectation for Tier 3 providers to follow the code of practice but they will be expected to comply with the regulations to a level which is appropriate and proportionate. In addition, Ofcom has stated that Tier 3 providers will not be part of the Tier 1 and Tier 2 compliance monitoring set out in their Draft general statement of policy under section 105Y of the Communication Act 2003[135]. However, Tier 3 providers will still be required to comply with their legal obligations, and Ofcom could use its powers to investigate potential breaches and take enforcement action where necessary. This supports our view that Tier 3 providers are unlikely to be disproportionately affected by the regulations and code of practice. There are multiple plausible explanations for the consistently low engagement from Tier 3 providers. Firstly, the low response rate suggests a lack of engagement with the regulations and its associated impacts, with some Tier 3 providers possibly believing that the new legislations do not directly apply to them. For those Tier 3 providers who do believe the legislation applies to them, they may not estimate significant cost impacts from the regulations and code of practice. Our view that the regulations and code of practice will not have a disproportionately large impact on Tier 3 providers supports this point. Finally, it may be the case that some Tier 3 providers lacked the capacity to respond to our cost survey, with smaller providers less likely to have compliance teams available to support a response to the survey.

8.15. In the period leading up to the public consultation, DCMS continued to engage with smaller businesses through trade bodies and industry-wide events. This engagement

[135] Annex 5: Draft general staement of policy under section 105Y of the Communications Act 2003 - https://www.ofcom.org.uk/__data/assets/pdf_file/0027/233568/annex-5-draft-s105A-Z-procedural-guidance.pdf

process included a roundtable event, jointly run by DCMS and TechUK, focussed on reaching smaller providers who have not previously been engaged with.

8.16. In addition to the costs analysis undertaken for smaller providers presented in this impact assessment, we have also outlined some of our qualitative findings below.

Box 5: Qualitative findings from Small and Micro businesses

We received three responses to our survey from small businesses and one response from micro businesses. All of the small businesses that responded are providers who hold code powers. The sole micro business that responded did not hold code powers. We set out in the section Number and type of businesses that will be affected that we assume these providers will incur higher direct costs than those without code powers on the basis they are more likely to own and operate network infrastructure. This assumption is backed up by the data in the survey responses. The vast majority of small businesses in scope of the Regulation do not have Code Powers (approximately 75%).

Based on the survey responses we found that some key costs for small businesses are:

- Familiarisation costs: Similar to larger businesses, small businesses flagged significant familiarisation costs.
- One-off costs: A small business will incur proportionately higher costs for fixed costs. Respondents mentioned some specific areas including testing, software development, management of permissions/authorisations and monitoring and analysis.

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

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

8.19. We also note that in absolute terms the most significant impacts of the regulations are likely to fall on larger businesses. This is in part due to the difference in size of the smallest and largest providers. It is useful to note that the seven largest providers hold 88% of the total fixed telecoms market in the UK. In the mobile network, this is even more pronounced, with just four network providers making up circa. 85% of the mobile network. The market share of each of these providers are shown in tables 20 and 21.

**Table 20: Mobile network market shares by subscribers at 31 December 2017**

| Provider | Market share |
|---|---|
| BT / EE | 28% |
| O2[136] | 26% |
| Vodafone | 21% |
| Three | 12% |
| Tesco Mobile | 6% |
| Virgin Mobile | 4% |
| TalkTalk | 1% |
| iD Mobile | 1% |
| Sky | 1% |
| Others | <1% |

Source: Statista[137]

**Table 21: Fixed network market shares by broadband subscribers at 2020**

| Provider | Market share |
|---|---|
| BT | 33% |
| Sky | 23% |
| Virgin Media | 20% |
| TalkTalk | 10% |
| Others | 14% |

Source: Statista[138]

8.20. The vast majority of UK telecoms networks are owned and managed by the nine providers above, all with a turnover above £1bnm. Therefore the large providers will be the ones who have to bear the majority of the costs involved in making the necessary changes to comply with the legislation.

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

8.22. Whilst we do not have data on the expected cost impact by firm size, we have considered the make up of small businesses that we have identified in the scope of the legislation. We found that these providers were less likely to hold Code Powers than large and medium providers and this may reflect the type of business with smaller numbers of SMEs operating network infrastructure. The consistently low engagement from smaller providers with this year's and last year's cost survey strongly suggest that SMEs will not

[136] O2 have Virgin Media have merged following the publication of this table

[137] UK: Mobile network market share 2018

[138] UK telecoms providers: broadband subscribers share 2020

be disproportionately affected by the incoming legislation. However, there are likely to be a number of SMEs who do incur significant costs, including one-off and indirect costs, as a result of the regulations and we consider both exemption and mitigation below.

8.23. Our estimates of the costs per business[139] from the legislation, split by tiers, supports our view that small businesses are unlikely to be disproportionately affected:

- our estimates suggest that Tier 3 providers will incur an average cost of £2.9m per firm
- this is contrast to Tier 2 providers where our estimates suggest an average cost per firm of £23.4m
- finally, Tier 1 providers are expected to have a significantly higher cost per firm from the legislation of £399m

8.24. The average legislation costs per firm are based on the total costs estimated over the 10 year appraisal period used in the impact assessments' cost benefit analysis. DCMS notes that the estimated cost per firm for Tier 3 providers is likely to be an overestimation. This is because the department believes several Tier 3 providers will not be significantly impacted by the regulations (for the reasons discussed earlier in this impact assessment) and the knowledge that Tier 3 providers will not be expected to follow the code of practice.

**Could SMBs be exempted while achieving the policy objectives?**

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

8.26. For small businesses, we do not consider an exemption to be appropriate. Customers of telecoms providers deserve appropriate levels of security to apply to their communications services irrespective of the size of the company providing the communications network and/or services. Smaller providers, which are not classified as micro businesses (turnover above £632,000 but less than £10.2 million), have the capacity to become regional telecoms providers serving thousands of customers. Therefore we believe it is proportionate for small businesses to be in scope of the regulations. During the consultation on the draft regulations and draft code of practice we did not receive significant objections in our approach to micro business exemptions.

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

[139] Total legislation cost per business calculation is based on total one-off, ongoing, familiarisation and reporting (Tier 1 and Tier 2 only) costs in this impact assessment divided by DCMS' estimate of the total populations in Tiers 1, 2 and 3.

technical expertise and higher relative familiarisation costs. Therefore, the Statutory Instrument will include an exemption for micro businesses.

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

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

8.29. To ensure measures are applied proportionately, the government intends to define three tiers of telecoms provider in the final code of practice.. A summary of the obligations of each tier and the level of oversight applied is below:

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

8.30. A disproportionate impact on Tier 3 providers, and thus on small businesses, is expected to be mitigated by no expectation to follow the detailed requirements set out in the code and a proportionality requirement which is built into the Act and limited oversight from Ofcom. In addition to this, under option 1, Tier 2 providers would have a longer implementation timetable and this could have an impact on both when these providers begin to incur costs and the level of costs they will incur. Tier 3 providers may choose to adopt the measures in the code of practice where these are relevant to their networks and services.

8.31. We do not anticipate that Ofcom will require Tier 3 providers to undertake any periodic reporting under this legislation. While Tier 1 and Tier 2 providers will likely be expected to produce annual reports of their compliance against the legislation and any deviation from the code of practice, this will not be expected of Tier 3 providers. According to the Deloitte report of the impact of FCA regulations on financial services firms, activities where small firms would save more cost than medium/large firms if rules were removed includes periodic reporting[140].

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

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

# 9. Wider impacts

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

## Competition assessment

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

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

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

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

### Downstream UK telecommunications market

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

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

9.7. In addition to BT, Virgin Media O2 operates a cable network that currently covers approximately 50% of the UK. In addition to BT and Virgin Media O2, there are many fixed telecoms retail service providers in the UK, including Sky and TalkTalk, along with various alternative infrastructure providers, including Hyperoptic, Gigaclear, KCOM and CityFibre who provide retail and/or wholesale services in discrete geographical areas.

**Will the legislation limit the number or range of suppliers?**

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

- significantly raises the costs of incumbent firms, causing them to exit the market;
- significantly raises the costs of new suppliers (including small businesses) relative to existing suppliers; and
- significantly raises the costs of some existing suppliers relative to other existing suppliers."[141]

9.9. We therefore consider each of these questions.

**Will the legislation raise the costs of incumbent firms?**

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

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

9.12. Large and medium sized providers that responded to our survey estimated potential one off costs of approximately 6% of turnover and annual ongoing costs of 2% of complying with the draft regulations on average. Although we expect that this will vary by type of provider. However, we also expect that implementing the regulations will deliver direct benefits to providers reducing the net cost.

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

9.14. In clarification meetings with Tier 1 providers, concern was raised around the proposed implementation timeframes for measures in the draft code of practice. Tier 1 providers stated the Tier 1 implementation timeframes would be challenging and costly to meet. Related to this, Tier 1 providers also suggested that smaller providers may become more reluctant to engage in business with Tier 1 providers due to the difference in implementation dates which might require smaller providers to comply with the requirements in the code of practice and regulations earlier due to their business with Tier 1 operators. Tier 1 providers stated that in this scenario they may be required to bear the additional cost of the smaller provider having to comply with the requirements earlier. Since these clarification meetings, DCMS have agreed to alter the implementation timelines, post consultation, for Tier 1 providers in our preferred option 1 as outlined in the 'Description of options considered' section. The amendment to the proposed

[141] Competition impact assessment Guidelines, Section 3.24.

implementation timeframe will allow additional time for implementation to Tier 1 providers which should mitigate the potential cost issue highlighted for Tier 1 providers.

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

**Will the legislation raise the costs to new suppliers?**

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

9.17. We note that the costs of implementing the regulations appear to be skewed towards one off costs. This could be indicative of significant change management processes and costs associated with changes to existing business processes and systems. These types of costs might affect new suppliers less as the regulations can be built into business process and system design from the outset.

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

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

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

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

**Relative impacts on existing suppliers**

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

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

9.23. In particular, option 1 mitigates the costs in implementing the regulations for smaller providers by delaying their implementation date. This delay means that smaller telecommunications providers would be able to delay implementation or implement over a longer period

9.24. We have also considered the relative impact on suppliers who are global providers. These suppliers may find it more difficult to implement UK-specific regulations where they differ from standards in other countries. This issue was specifically highlighted in a clarification meeting with a telecoms provider whose competitors are located in the United States and the European Union. The provider outlined the risk of its overseas operations being negatively impacted by the new security standards due to come into force in the UK. It was argued that resource would need to be diverted away from overseas operations in preparation for the incoming regulations and code of practice.

9.25. However, we note that a large number of suppliers operate globally yet still meet the needs of specific markets and serve a vast array of providers, many of whom have different needs. Global suppliers are likely to assist providers to meet legal requirements as far as possible. In the global context, we note that the regulations are innovative in setting out security requirements for telecommunications providers in detail. However, other countries are planning similar measures, as noted in section 5, which will impact the market globally, reducing any barrier to entry into the UK market that the new security framework may create.

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

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

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

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

9.29. In addition to this the security framework has been designed to balance the need for a level of prescription in setting out the security requirements with a mechanism for providers to follow their own approach to implementing the draft regulations.[142] This approach recognises the need to balance the potential benefits of providers being able to innovate and react to change against the need to meet a level of security requirements.

9.30. In our survey of PECN and PECS we asked providers how they plan to comply with the draft regulations. Only 20% expected to comply by implementing the code in all areas; the vast majority indicating that they would depart from the code in some way.

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

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

**Table 22: Q2.3b - If you plan to implement the requirements set out in the draft code of practice where possible but plan to set out your own approach for some areas, please select the reason(s) for this approach.**

| Answer | % |
|---|---|
| Difficult to implement requirements set out in the draft code of practice due to legacy systems | 23% |
| To be more cost-effective | 20% |
| To maximise network security | 31% |
| To align with our company's global approach | 14% |
| We prefer another approach, please explain | 11% |

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

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

**Impact on innovation**

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

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

9.35. In clarification meetings following the cost survey deadline, telecoms providers outlined the risk of prioritising resource away from innovation to support compliance with the regulations and code of practice. This may delay innovation for some telecoms operators. In addition, other regulatory changes in the telecommunications sector e.g, Designated Vendor Direction were highlighted as factors which may challenge innovation further with specific references made to 5G standalone and full fibre network investment. In contrast, other telecoms providers highlighted the need for incentives, such as the new telecoms security framework, to drive innovation in the area of security and resilience in the long term. One provider in particular stated that innovation would be a 'natural by-product' of the regulations and code of practice. Standardisation across network signalling requirements was suggested as a potential area for opportunity. Nonetheless all telecoms providers did state that it would take time to understand how the new security requirements will impact innovation. In relation to this, DCMS has committed to reviewing

and updating the code of practice and regulations to consider technology and innovation in this sector.

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

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

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

## Equalities Impact Assessment

9.38. We do not consider there to be any disproportionate impacts to groups with protected characteristics. The costs of this legislation fall on businesses only so do not have an impact on any protected groups. The benefits to society arise from the reduction in the impact of security compromises for telecoms providers. This is likely to benefit any consumer in the UK with access to a mobile or broadband service. This does not preclude any protected groups since every home and business in the UK has the legal right to request a decent, affordable broadband connection under the Broadband Universal Service Obligation (USO)[143]. The benefits accruing from the deployment of 5G use cases that require a reliable and secure 5G network is expected to accrue mostly to businesses. While a small proportion of consumers have access to 5G already[144], it is widely considered that the majority of 5G benefits will accrue to businesses. While consumers will benefit from faster speeds, more availability and consumer-focused use cases such as smart home IoT devices, the real gains come from the benefits of increased efficiency and productivity in almost every sector. As such, we do not consider protected groups to be either positively or negatively impacted by this legislation compared to the UK population as a whole.

9.39. It is worth noting that a small proportion of the UK are digitally-excluded. According to Ofcom's latest 'Adult's Media Use and Attitudes' report, 6% of households did not have access to the internet at home as of March 2021 and a further 1% of adults aged 18+ had access to the internet at home but did not use it. In particular, the groups more likely not to have internet access at home – and therefore, to be more at risk of digital exclusion – were those aged 65+ (18%), those in DE households (11%) and those who were most financially vulnerable (10%)[145]. However, we do not consider that this legislation is increasing the disadvantage of those who are digitally excluded. The outcome of the policy is ensuring the security and resilience of the existing and future telecoms networks in the UK. While we expect the legislation to enable the growth of a number of 5G use cases, the benefits of these fall on businesses rather than consumers for the most part and so would not further disadvantage those who are digitally excluded.

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

[144] 5G services available at around 3,000 sites. EE, O2, Three and Vodafone first started rolling out 5G in the UK in 2019 and have continued to extend their networks across the UK. Many 5G sites are in busy areas and are providing enhanced capacity to existing mobile data services. Of all 5G sites that have been deployed, 87% are in England, 7% in Scotland and 3% in both Wales and Northern Ireland. This split broadly reflects the national distribution of all mobile traffic across the UK. Connected Nations report 2020, Ofcom

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

# 10. A summary of the potential trade implications of measures

### Impact on trade: network and service providers

10.1. The Electronic Communications (Security Measures) Regulations include requirements in Regulation 3, Regulation 5 and Regulation 9 that are intended to mitigate the risk to the availability of telecoms networks within the UK in the event of disruption to international connectivity or offshore technical and operational support. These requirements are designed to ensure that UK networks remain available, particularly in the event of any impact to international connectivity, as well as limiting the ability for malicious insiders, based outside the UK, to damage UK networks. They also ensure that copies of data needed to rebuild network capabilities (but not content) are retained within the UK, though such copies may be retained elsewhere too.[146]

10.2. The regulations also include requirements to protect monitoring and analysis tools by ensuring that providers account for location-related risks. The schedule in the regulations lists certain high-risk locations where security capabilities that monitor and analyse UK networks and services must not be located. Security capabilities must also not be accessible from those locations. Where providers host capabilities in other non-UK locations, they must identify and reduce the risks of security compromise occurring as a result of monitoring and analysis tools being stored on equipment in those locations.[147]

10.3. The following duties on providers are included in the regulations:

- to ensure that the network provider is able, without reliance on persons, equipment or stored data located outside the United Kingdom, to identify the risks of security compromises occurring,
- to ensure that the network provider is able to identify any risk that it may become necessary to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom. [148]
- to ensure that, if it should become necessary to do so, the network provider would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom.
- if the tools are stored on equipment located outside the United Kingdom, take measures to identify and reduce the risks of security compromises occurring as a result of the tools being stored on equipment located outside the United Kingdom.
- to ensure that the tools— (a) are not capable of being accessed from a country listed in the Schedule, and (b) are not stored on equipment located in a country so listed.
- to create or acquire and to retain within the United Kingdom— (i) an online copy of information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service, and (ii) so far as is proportionate, an offline copy of that information

[146] [Relevant regulations to be numbered once final regulations have been signed off by Ministers]
[147] [Relevant regulations to be numbered once final regulations have been signed off by Ministers]
[148] Draft Electronic Communications (Security Measures) Regulations, section 5, point 3(h)

10.4. Additional detailed guidance relating to these regulations is set out in the code of practice. This is contained within chapters two, four and eight of Section Two; and corresponding measures within Section Three.

10.5. The government has further assessed and updated the regulations based on the feedback received to the public consultation from a broad cross-section of stakeholders who could be impacted. This includes requests to clarify the scenarios under which certain services must be maintained from within the UK, and more specific descriptions of the type of services that should be maintained in those scenarios.

10.6. Inward investment and R&D will be key to developing secure, efficient 5G services within the UK. The final regulations will ensure that businesses have certainty on the level of security and resilience they need to offer. Clarity on the scenarios and types of critical services that should be maintainable from within the UK will ensure that investment into the UK's telecoms critical national infrastructure puts next generation services on a sustainable footing.

**Impact on trade: third party suppliers**

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

# 11. Justice impact test

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

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

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

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

# 12. Monitoring and evaluation

12.1. Since the publication of the consultation-stage impact assessment, a monitoring and evaluation methodological approach has been developed further. Post-implementation review is to be carried out by October 2027. Ofcom's spending objectives and its plans to evaluate progress against these were agreed as part of the business case. These are set out below in Table 23.

12.2. DCMS will monitor factors such as the number of incidents reported and the number of 5G and full fibre network rollouts. It should be noted however, that such top down data may lead to misleading conclusions of the true effect of the regulations. This is due to the difficulty in correctly identifying the impact of the regulations on trends such as the increasing number of cyber security incidents as well as 5G and full fibre rollout. In addition to the trend of increasing cyber security incidents, an increase in incident numbers could also show an improvement in cyber security as better cyber security can lead to more breaches and potential breaches being detected. This would mean reporting on such top down metrics could potentially be misleading in evaluating the policy, but still an important metric to collect.

**Table 23: Ofcom's provisional post-implementation and evaluation plans**

| Spending Objective | What sources of data will be used to understand if an objective has been completed? | When/How will it be evaluated? |
|---|---|---|
| 1. **Skills/resources**: Ensuring Ofcom has resources in order to deliver against its enhanced responsibilities under the Telecommunications (Security) Act. | Number of roles filled, outstanding vacancies | Ongoing evaluation with Ofcom's Operations team, third-party recruitment partner and specialist head-hunters. Ofcom to internally review progress on a monthly basis on roles filled against the target headcount. |
| 2. **Cyber incident reporting**: Significant cyber security incidents are detected by providers, and reported to Ofcom in a timely manner, even when there is no immediate impact on customer service. Where reported incidents raise potential compliance concerns, Ofcom will investigate the causes and responses to the incident. | Incidents are reported to Ofcom and reports are then captured on its Incident Reporting Information Management System | A monthly review process is carried out of incidents reported to Ofcom. A triage is then done to establish whether any reported incidents raise potential compliance concerns. This will include checking against compliance reports. |

| | | |
|---|---|---|
| 3. **Resilience guidance and reporting**: Ofcom publishes industry guidance on its compliance expectations in relation to the availability and resilience aspects of security. Significant availability incidents are reported to Ofcom in a timely manner, and where they raise potential compliance concerns, Ofcom will investigate the causes and responses to the incident. | Incidents are reported to Ofcom and reports are then captured on its Incident Reporting Information Management System | A monthly review process is carried out of incidents reported to Ofcom. A triage is then done to establish whether any reported incidents raise potential compliance concerns. This will include checking against compliance reports.<br><br>On the resilience guidance, Ofcom will work with the EC-RRG[149] to obtain their input and ensure it captures the necessary information. Ofcom will also carry out a public consultation with industry before publishing the final version. |
| 4. **Enforcement**: Where Ofcom has concerns about regulatory compliance it will take appropriate enforcement action. | As Ofcom reviews compliance reports from industry, it will assess the steps taken/not taken by communications providers in order identify priority areas of concern. Ofcom will use this to form a view on whether to pursue enforcement action.<br>Details of enforcement action are published on Ofcom's website. | Ongoing evaluation will be undertaken to understand whether the correct enforcement action has been taken.<br><br>In line with clause 14 of the Act, the Secretary of State must review the effectiveness of the legislation no more than five years after commencement. Ofcom will input into this review, drawing on its experience of compliance monitoring. |
| 5. **Compliance monitoring**: Ofcom will, over time, build a detailed understanding of the relevant network and services currently operated, and planned, by major providers. This will include understanding the key security risks faced and the implemented and planned security measures, and how these align with, or differ from, the advice in the relevant DCMS Code(s) of Practice. | Responses to information requests, follow up meetings with providers, findings from assessment notices (e.g. TBEST[150], interviews, tests). | Ofcom will undertake ongoing evaluation of the action industry is taking and how it is responding to compliance incentives.<br><br>In line with clause 14 of the Act, the Secretary of State must review the effectiveness of the legislation no more than five years after commencement. Ofcom will input into this review, drawing on its experience of compliance monitoring. |

[149] Electronic Communications Resilience and Response Group - Further information about which can be found at: https://www.gov.uk/guidance/electronic-communications-resilience-response-group-ec-rrg

[150] A Penetration Testing Scheme run by Ofcom and NCSC to simulate attacks on operators networks.

| | | |
|---|---|---|
| **6. Reporting to Secretary of State**: Ofcom will share relevant information arising from its enforcement of the regulations with Government. This will include: informing the Secretary of State of any security risks or compromises that raise serious concerns relating to matters (including national security, public safety, and the economy of the sector); and regular reporting to Secretary of State on the providers' compliance with the legislation and adherence to the Code(s) of Practice. Ofcom will also undertake monitoring of providers' usage of high risk vendors when directed to do so. | Reports to Secretary of State on industry compliance with security framework and monitoring reports on high risk vendors<br><br>Reports to the Secretary of State under clause 4 of the Act. | Ofcom will work with DCMS to understand if there is any feedback from the Secretary of State on the reports. |
| **7. Transparency**: Ofcom will undertake monitoring and enforcement of the Regulations with an appropriate degree of transparency, in line with its general duty to act transparently, and with the specific provisions in the Act. | Publication of procedural guidance, summaries in Ofcom's annual infrastructure report (Connected Nations) of the level of security within the sector and publication of regulatory breach decisions. | Consultation responses to procedural guidance; relevant Parliamentary scrutiny, including select committee hearings. |

12.3. In addition to Ofcom's post-implementation and evaluation plan, DCMS may obtain data from year 1 onwards related to the regulations and code of practice following implementation. This may include data on:

- The number and nature of enforcement notices issued by the regulator
- The compliance rate in relation to the regulations and code of practice
- The amount spent by telecoms providers to comply with the regulations and code of practice
- National statistics on the prioritisation of cyber security in telecoms companies
- Qualitative data on the behaviour of telecoms providers before and after the implementation of the regulations and code of practice.

12.4. These measures can be used in the upcoming years as proxies to ascertain whether the regulations are having their desired impact. For example, enforcement action data can help indicate whether telecoms providers are not complying with the regulations, while direct expenditure to comply with the regulations may indicate telecom provider's intentions in regards to compliance. An agreement will be arranged before an appropriate data collection strategy is finalised. If the data above (or similar) is collected, analysts will be able to utilise methods to estimate the risk reduction from the improvements that the regulations have generated on cyber security.

12.5. To further help determine whether the regulations and code of practice have been fit for purpose, we may develop hypothetical outcomes under our 'Do nothing' option' where the regulations and code of practice are not implemented. These scenarios will help estimate the impacts of this hypothetical scenario including the effect on key stakeholders. This work should build upon the benefits analysis detailed in section 6, estimating how many more security compromises may have occurred and 5G use case benefits lost in absence of the regulations. The data, metrics and approaches outlined in this section can be used to assess whether the regulations and code of practice have achieved the policy objectives outlined in this impact assessment.

12.6. The rapid changes in technology and innovation in this sector pose a challenge to an effective monitoring and evaluation programme being undertaken. As a result, DCMS commits to reviewing and updating the final monitoring and evaluation framework in line with any significant updates made to the code of practice or regulations. The code of practice and regulations will be reviewed regularly and will be updated as new threats emerge, technologies evolve or to address security vulnerabilities identified through compliance reporting.

12.7. As explained in our Economic Impact - benefits section, DCMS can not confidently estimate the proportion of the calculated benefits that could be attributed to the legislation. As a result, it is important that our monitoring and evaluation framework attempts to quantify the magnitude of the benefits (security compromises avoided and 5G use cases) outlined in this impact assessment as well as other benefits derived from the policy which may be uncovered in future. To support this work, DCMS analysts should attempt to find more robust evidence on the costs of security compromises for Tier 3 providers specifically but also for Tier 1 and Tier 2 operators. This data paired with estimates for the number of avoided security compromises from the policy will help to quantify these benefits. In regards to the 5G use cases highlighted, the department should consistently look to update the evidence base around the quantitative benefits from these new technologies. This includes further work to investigate the relationship between secure and resilient telecoms networks and the economic benefits produced from 5G use cases. Taking such evidence and estimating a proportion of the benefits attributed to the regulations and code of practice will remain challenging however. Despite this, further work in this area will help us to revisit the estimated net benefit for the legislation in future.

12.8. The impact assessment contains some evidence gaps primarily due to the low response rate from Tier 2 and Tier 3 providers. Consequently, the department should continue to regularly assess the impact of the new security framework on Tier 2 and Tier 3 providers once the policy has commenced. This could be in the form of surveys to a random sample of providers or follow-up meetings with a variety of Tier 2 and Tier 3 providers to better understand the realised costs (and other impacts) to some operators from implementing and complying with the regulations and code of practice.

**How is the current system monitored?**

12.9. Ofcom has the following powers with respect to monitoring public communications providers under legislation currently in force:
- Ofcom may require providers of PECN and PECS to submit to, and pay for, an audit of the measures they are taking to comply with the obligations; and
- Ofcom can use the information gathering and enforcement provisions in the Communications Act to investigate, rectify, and penalise any infringement of these obligations.

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

12.11. The guidance that is currently published by Ofcom to guide communications providers on their security and resilience obligations has been updated once since its publication in May 2011.[151]

12.12. With reference to the updated guidance, Ofcom notes that 'Because of the dynamic nature of the telecoms market, and the changing threats to security and resilience it faces, we will continue to review this document regularly, and if required, update it again.'[152]

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

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

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

12.15. 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.'[153] Such changes in technology or the adoption of technology can rapidly change the security landscape of the telecommunications sector.

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

[151] Ofcom's current guidance security requirements in sections 105A to D of the Communications Act 2003 was published in 2017. This guidance replaced previous guidance which was published in May 2011.
[152] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance
[153] The Review, page 24.

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

**How will the new security framework be monitored?**

12.18. The new security framework will include a set of security duties in the Communications Act 2003, a set of regulations and a code of practice.
12.19. The contents of the code of practice will be reviewed on a regular basis to ensure it keeps pace with the latest threats and evolving technology.
12.20. The NCSC will inform the government of where new threats and vulnerabilities lie based on its analysis and classified intelligence.
12.21. Alongside this, Ofcom must publish a security report after the end of each reporting period containing information and advice that Ofcom considers will assist the government with forming policy. This will include information about whether providers have complied with their duties under the Act and acted in accordance with the code. Access to this information will allow the government to understand how well the new framework is working and where changes to the code need to be made.
12.22. Box 6 below sets out an extract from the Telecommunications (Security) Act which amends the Communications Act 2003 to add section 105Z 'OFCOM reports on security'. This section sets out the contents of the security report that Ofcom must prepare and send to the Secretary of State.

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

105Z OFCOM reports on security

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

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

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

(4) A security report must in particular include—

(a) information about the extent to which providers of public electronic communications networks and public electronic communications services have complied during the reporting period with the duties imposed on them by or under sections 105A to 105D, 105I to 105K, 105N(2)(a) and 105O;
(b) information about the extent to which providers of public electronic communications networks and public electronic communications services have acted during the reporting period in accordance with codes of practice issued under section 105E;
(c) information about the security compromises that OFCOM have been informed of during the

reporting period under section 105K;
(d) information about the action taken by OFCOM during the reporting period in response to security compromises they have been informed of under section 105K;
(e) information about the extent to which and manner in which OFCOM have exercised the functions conferred on them by sections 105I and 105L to 105V during the reporting period;
(f) information about any particular risks to the security of public electronic communications networks and public electronic communications services of which OFCOM have become aware during the reporting period;
(g) any other information of a kind specified in a direction given by the Secretary of State.

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

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

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

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

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

12.27. The Review will be informed by all of the data sources set out above. This will include data collected by Ofcom on compliance with the code of practice which will provide DCMS with information on how Tier 1 and 2 providers are implementing the code and data on security compromises reported. Where required DCMS will seek additional data.

# 13. Glossary and Abbreviations

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

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

AR - Augmented reality

ADSL technology - Asymmetric digital subscriber line technology

CA - Communications Act 2003

CNI - Critical National Infrastructure

DCMS - Department for Digital, Culture, Media & Sport

FTTP - Fibre to the premises

GVA - Gross value added

HRV - High risk vendor

IoT - Internet of things

ISPA - Internet Service Providers' Association

MANO - Management and Organisation

MNO - Mobile Network providers

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

MVNO - Mobile Virtual Network providers

NCSC - National Cyber Security Centre

NFV - Network Function Virtualisation

NFVi - Network Function Virtualisation Infrastructure

NSA - Non-standalone

Ofcom - Office of Communications

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

PECN - Public Electronic Communications Network

PECS - Public Electronic Communications Service

SA - Standalone

VoIP - Voice over IP

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

### Remote medical examination (Economic Benefit: £6.4bn)

1.1. The Ericsson report states the key dimensions of 5G in enabling remote medical examination and monitoring:
- 'Enabling high definition video streaming over mobile networks
- Offering high enough availability and reliability to constantly monitor critical patient health parameters
- Being secure enough to adhere to sensitive patient data regulations.'[154]

1.2. A 2019 report from Cambridge Wireless states that '5G technology brings the opportunity for paramedics to transmit images, data and detailed information from ambulances *en route* to the hospital to prepare doctors for treatment. Equally, high-quality video links may allow paramedics to conduct emergency treatment or assess and diagnose patients at the scene with the assistance of an on-line specialist.'[155]

1.3. O2 published a report on the value of 5G in May 2018 ('the O2 report'), which estimates that high quality and secure tele-health video conferencing will allow people to conduct GP consultations from their smartphone or other smart devices. This will save individuals an estimated 3.3 hours per year, saving £1.3bn in lost productivity through workplace absence[156]. 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.'[157]

1.4. The development of remote healthcare is of even higher importance due to the Covid-19 pandemic. This has led to a faster uptake of remote medical examination than anticipated. Recent data collected by the Royal College of GPs showed that at the peak of the pandemic, up to 70% of consultations were carried out by phone or video call[158]. Reliable, 5G mobile networks are the catalyst for this remote approach to continue and evolve. For example, 5G-aided remote CT scans were used to diagnose COVID-19 patients in China[159].

1.5. Analysts at Global Market Insights predict the use of telehealth will triple by 2025, fuelled largely by 5G[160]. The same report states that the 'Teleconsultation service market is expected to grow at 18.9% CAGR across the forecast timeframe.'[161]. This does not account for the acceleration enabled by Covid-19. We have based our analysis on pre-Covid figures as the growth rates due to Covid are not fully established.

1.6. Our model of the economic benefits of remote medical examination starts with the £1.3bn benefit expected in 2026. This is based on the assumption that 5G penetration

---

[154] Ericsson's 5G Business Potential report

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

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

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

[158] Around 7 in 10 patients now receive GP care remotely in bid to keep patients safe during pandemic, says RCGP, 30 April 2020

[159] 5G-aided remote CT scans used to diagnose COVID-19 patients, 28 February 2020

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

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

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

**Remote health monitoring (Economic Benefit: £6.6bn)**

1.7. In the context of the Covid-19 pandemic, much attention has focused on 5G's potential to support telehealth services. 5G offers the potential of moving these interactions a big step forward by, for example, adding sensors and virtual reality to teleconferencing, enabling healthcare workers to remotely monitor vital signs during calls. 5G can transmit sizeable data packages, testing patients with conditions for changes in their heartbeat, blood sugar and blood pressure multiple times a day using cloud-linked scanners[162].

1.8. The O2 2018 report estimates that health monitoring devices will reduce hospital readmissions by 30% by 2025 and save £463m in NHS costs as a result (through a combination of decreasing bed occupancy and giving hours back to hospital staff). Remote health monitoring will also save local councils £890m through reduced social care budgets[163]. Taken together, this produces a potential annual benefit of £1,353 million by 2025[164]. This is a lower estimate than the one produced in the 2017 study by the Iqvia Institute for Human Data Science, which states that the use of Digital Health apps could achieve annual cost savings of £2 billion[165].

1.9. A Deloitte report in 2018 estimated that the Internet of Medical Things market - defined as medical devices that can generate, collect, analyse, transmit and store large amounts of health data - is expected to grow at a compound annual growth rate (CAGR) of 30.8% from 2017 to 2022[166].

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

**Connected and autonomous cars (Economic Benefit: £12.5bn):**

1.11. TechRadar stated in June 2019 that ‘5G could be the key to making self-driving cars commonplace. For them to work most effectively they need to be able to rapidly send and receive data to and from other cars, smart roads and more, which requires a speedy network, low latency, lots of bandwidth and high reliability. 5G promises all of that.’[167]

---

[162] 5G in healthcare, PwC, 2020

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

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

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

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

[167] 10 things 5G can do that 4G can’t

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

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