Electronic Communications (Security Measures) Regulations

Lead department	Department for Digital, Culture, Media and Sport
Summary of proposal	A proposal to establish a robust security framework for 5G and full fibre networks. The regulations set out the priority security requirements for providers of public telecommunications networks and services (PECN and PECS), and the actions that must be taken to achieve them.
Submission type	Impact assessment (IA) – 23 June 2022
Legislation type	Secondary legislation
Implementation date	September 2022
Policy stage	Final
RPC reference	RPC-DCMS-4474(4)
Opinion type	Formal
Date of issue	03 August 2022

RPC opinion

Rating[1]	**RPC opinion**
Fit for purpose	The IA presents a good argument for intervention but should discuss all options that have been considered to date in more detail. The SaMBA includes details of the small and micro businesses (SMBs) likely to be affected, as well as addressing exemption and mitigation, but it should include more discussion of the additional impacts if option 2 were implemented. The Department has used the consultation and on-going stakeholder engagement to strengthen the evidence underpinning the analysis. The Department has included a well-rounded consideration of the wider impacts of the policy, including a discussion on the impacts to innovation. The Department include a detailed monitoring and evaluation (M&E) plan to assess the impact of the policy, and build upon the range of monitoring activities that are already being undertaken by Ofcom in this area.

[1] The RPC opinion rating is based only on the robustness of the EANDCB and quality of the SaMBA, as set out in the Better Regulation Framework. RPC ratings are fit for purpose or not fit for purpose.

Business impact target assessment

	Department assessment	RPC validated
Classification	Qualifying regulatory provision	Qualifying regulatory provision
Equivalent annual net direct cost to business (EANDCB)	£470.5 million	£470.5 million *(2019 prices, 2020 pv)*
Business impact target (BIT) score	£2,352.5 million	£2,352.5 million
Business net present value	£-4,102.9 million	
Overall net present value	£-4,103.9 million	

RPC summary

Category	Quality[2]	RPC comments
EANDCB	**Green**	The IA identifies a range of impacts for the proposals and correctly identifies the direct impacts for inclusion in the EANDCB for validation. The Department should seek to fully monetise the benefits discussed, such as the reduction in the cost of security incidents and the wider benefits of the proposals (e.g. the economic benefits of 5G and full fibre, and the benefits to consumers of improved security).
Small and micro business assessment (SaMBA)	**Green**	The IA includes detailed qualitative discussion of the potential impacts on small and micro businesses (SMBs), if included in scope. The IA considers the market structure of the sector and provides an exemption for micro businesses and mitigation for small businesses. It would be improved by considering what additional or amplified impacts there may be, if option 2 were implemented, as well as if the expected costs can be presented with respect to turnover for SMB providers.
Rationale and options	**Satisfactory**	The Department sets out the rationale for intervention clearly, presenting market failure arguments and citing national security and associated resilience risks. The IA sets out the options considered at this stage, however only the preferred option and the 'implementation plus' (option 2) are considered in any detail. The alternative options, including a non-regulatory option, should be discussed in greater detail. The IA would also benefit from an analysis of option 2, for comparison with the preferred option.
Cost-benefit analysis	**Satisfactory**	The methodology and assumptions used in the IA are clearly set out and are supported by the available evidence. The Department has sought to strengthen the evidence base as much as possible through on-going engagement, while acknowledging and making clear the limitations of the evidence gathered.
Wider impacts	**Good**	The IA references the potential impacts on innovation throughout and also addresses this in a standalone section. A competition assessment, which focusses on the downstream impacts and limitations upon suppliers, is also included. In

[2] The RPC quality ratings are used to indicate the quality and robustness of the evidence used to support different analytical areas. Please find the definitions of the RPC quality ratings here.

		addition, the IA considers the impact on international trade, international networks and service providers more broadly.
Monitoring and evaluation plan	**Good**	The Department commits to review the Code of Practice as it develops, to keep pace with potential new threats and developments in technology. The IA includes a detailed provisional plan for developing a post-implementation review (PIR), that will be run by Ofcom and build upon the range of monitoring work that they currently undertake.

Summary of proposal

The Electronic Communications (Security Measures) Regulations are at the core of the new telecommunications security framework, which will deliver effective and enforceable security for telecommunications.

The IA explains that the introduction and deployment of 5G and full fibre networks across the country is a primary objective of the Government. The UK seeks to become a world leader in the rollout of 5G technology and the regulations to be introduced here, are seen as a key step in enabling this. However, 5G presents new risks that have not been present with its predecessors 3G and 4G.

The Department considers three options including the do-nothing baseline but only discusses the impacts of their preferred option and the 'implementation plus' option, in any detail. The options included in the IA are:

- **Option 0** - *Do nothing*;
- **Option 1** – *The specific security requirements are set out in regulations* (The Preferred Option). These are applied appropriately to providers of public telecommunications networks and services (PECN and PECS) in different ways, reflecting the different characteristics of network security compared to service security. Implementation is phased by date according to turnover of the provider; and
- **Option 2** - *Implementation Plus*. The specific security requirements are set out in the regulations as they are in the preferred option, however the date of implementation of the policy does not vary for different providers; the guidance setting out a single set of implementation dates applying to all providers (e.g., tiers 1, 2 and 3).

The preferred option sets out a new security framework with a strengthened set of overarching security duties that providers must adhere to, alongside specific requirements for providers and a code of practice.

The IA identifies the direct costs which include initial familiarisation costs for all network providers, one-off implementation costs to network providers, the on-going costs to maintain new systems put in place, and the cost of compliance reporting by providers. There is also discussion of the indirect costs including monitoring costs to Ofcom (the regulator), as well as the indirect costs to the supply chain and consumers, primarily due to the potential of any increase in costs to providers being passed through. The benefits of the policy are the improved security to the network, with the potential reduction in cyber security incidents, while also helping to facilitate the introduction of new technology and innovation. The IA, in paragraph 1.5 and table 1, note the impact of RPC scrutiny at various stages upon the development of the final IA.

EANDCB

Direct and indirect impacts

The Department correctly identifies and attributes the direct and indirect costs to business, providing a robust figure for the EANDCB of the preferred option. The IA attributes all monetised costs to firms across the three tiers from complying with the new requirements as direct impacts. Additionally, the Department correctly identify that the costs to Ofcom will be indirect costs to business (therefore out of scope of the EANDCB). The IA would have been improved by considering the relative scale of the expected costs, to the level of profits that providers typically make.

Un-monetised impact(s)

The IA identities a broad range of impacts for the policy. However, not all impacts identified have been monetised, such as any costs that may be passed through (which is discussed in detail qualitatively) and the economic benefits, arising from the reduced costs from security incidents and from the use of 5G. The IA would be improved by attempting to monetise these impacts where possible, in particular the economic and wider benefits, given the scale of the costs of implementing the policy.

SaMBA

Scope

The IA sets out the structure and market shares for the fixed telecoms and mobile network markets, which suggests SMBs represent a small proportion of the markets that will be affected. In addition, it establishes the Department's understanding of which tier SMBs are likely to be in, and therefore what requirements they will face. While small providers will not be required to comply with all of the new requirements, as they are assumed to most likely be in tier 3, the Department has included stakeholder feedback which sets out how these firms are likely to be impacted, if they were required to comply.

The Department do not expect small providers (which are considered separately because micro businesses are exempt) to be disproportionately impacted by any costs that they will face, providing an appropriate explanation to support this determination. The IA would be improved by the inclusion of a quantitative measure to substantiate this conclusion (e.g., costs as % of business turnover).

The Department acknowledge the difficulty in attaining robust evidence on the impacts to SMBs, while providing appropriate caveats to the evidence they have been able to gather. The IA states that while the evidence gathered may provide an indication of the likely costs to small providers, it cannot be assumed to be the case for all. In addition, the IA notes the additional efforts, such as the roundtable engagement event, that was made to gather evidence on SMBs. The IA would have been improved, by including some discussion of what impacts option 2

(implementation plus) may have on SMBs if it were to be implemented and whether this would disproportionately impact them.

Exemption and mitigation

The IA sets out that an exemption will apply to micro businesses, because their low market share, means any security incident would likely not have a significant impact for the overall market. Furthermore, the IA notes, in paragraph 4.13, that if the requirements were applied to micro businesses, they would likely result in a disproportionate financial impact. Meanwhile, the Department explains that an exemption for small businesses is not appropriate, in order to provide protection for customers.

The Department has also considered mitigation for small businesses, and given these firms are likely to be tier 3 providers, they will not be expected to follow the detailed requirements that will be set out in the Code of Practice. However, the analysis indicates that despite their exemption from the new requirements, all providers are anticipated to undertake some familiarisation with the new policy and therefore small businesses will incur some initial costs.

Rationale and options

Rationale

The IA sets out a clear rationale for intervention, which is supported by the identification of market failures. It argues that a new 5G network could have the potential to be a national security risk, particularly given the degree of reliance on it. The introduction of a 5G network poses different national security risks to those under current 3G/4G networks.

The IA cites points raised in the recent report (The Review), demonstrating how the telecoms market is not currently incentivising good cyber security, as there is:

- insufficient clarity on cyber standards;
- poor incentives to internalise the costs/benefits of security;
- insufficient market mechanisms, as customers don’t value security as much as the cost to them or the quality of service; and
- complexity in delivering it.

The Department also goes further in explaining why government is best placed to intervene. In addition, the IA includes clear objectives for the policy and also makes reference, in paragraph 1.13 to the international policy context of relevance to this legislation. The IA would have been improved by outlining more of the evidence on why consumers of telecoms services do not place a high value on security.

Options

The IA briefly lists the range of options that were considered throughout the policy making process, including both those formally considered in the IA, as well as other

options (such as a non-regulatory option to produce best-practice guidance) that have since been discarded. However, only the preferred option, of setting out specific security requirements in regulation, has been discussed in detail (with a clear summary presented in Box 3) and quantification of the impacts from its introduction been included.

While the IA provides explanation for their removal, the IA would be improved by retaining those additional options that were considered previously. Discussing the potential impacts of these other options, and quantifying where possible, would provide an illustration of the effects that respective options may have and that the preferred option provided the best outcome. In addition, the IA would be further improved by also seeking to quantify and discuss in more detail option 2 (implementation plus), to assist in explaining why this option has not been chosen.

Cost-benefit analysis

Evidence

The IA makes use of the available evidence, and relies heavily on the data gathered during consultation (during the development of both primary and secondary legislation), as well as on-going stakeholder engagement. The IA includes detailed discussion of the stakeholder engagement used to further refine the evidence where possible, including the amending of survey questions based on learnings from prior engagement, to improve the quality of responses.

The Department clearly explain the limitations of, and the uncertainty in, the evidence they use, in particular the survey responses and its use in the analysis. The Department should provide more detail on the range of responses received across the three tiers of affected businesses. Table 2 currently only details the rate of responses received and would benefit from providing context on the respective sizes of the tiers in question.

Analysis

The IA stratifies public telecom providers into three distinct tiers, based upon turnover: those with turnover greater than £1 billion (tier 1), those with turnover between £50 million and £1 billion (tier 2), and those with turnover less than £50 million (tier 3). The analysis uses this segmentation as the basis for attributing the different levels of cost to account for the different capability and operating practices of these firms. The Department clearly explain and set out the calculations that have been made to estimate the relevant impacts. The RPC commend the Department for undertaking break-even analysis to illustrate the level of reduction in security incidents necessary to offset the expected costs. The break-even analysis concludes that over 100% of the estimated direct benefits need to be realised to cover the costs. This illustrates the importance of quantifying and including the full range of benefits which have been identified but not all quantified.

Assumptions, risk and uncertainty

The IA makes several key assumptions within the analysis. The Department acknowledges the limitations of some of the cost estimates which rely on the limited survey responses gathered during consultation and on-going stakeholder engagement, and how this may lead to overestimation of costs. The Department has provided ranges, as appropriate, and sensitivity analysis to illustrate the potential variance in the scale of these uncertain impacts. The Department has used the on-going engagement with industry to thoroughly test the key assumptions and refine these as appropriate.

Wider impacts

Innovation

The IA includes a section on the impacts to innovation, where it discusses feedback that the Department received from stakeholders on how complying with the proposals would limit their ability to be innovative by diverting resource away from innovation. While the IA does well to address the impact upon innovation for firms directly affected by the measure, the IA would benefit from the inclusion of the expected, or potential, gains to productivity and innovation in general (including in areas such as cyber-insurance) that this policy would facilitate. The IA could also explore in greater detail whether the regulations give the providers the flexibility to appropriately develop technology in a fast-moving market.

Competition

The IA includes a well-developed competition assessment. Within this topic the Department has addressed the impact on the downstream UK telecoms market, as well as the impact on current suppliers and barriers to entry for new ones. The competition assessment would benefit from discussing whether the proposed difference in implementation timescales between options 1 (the preferred option) and 2, will have any impact on competition, given that latter proposes a consistent timeframe for both tier 1 and tier 2 providers. The IA concludes that barriers to entry from global suppliers will not be increased as many other countries are planning similar measures. The IA could be improved by discussing whether the application of the different regulations, according to turnover size, distorts competition between different provider groups, for example whether there are now additional barriers to providers moving from Tier 3 to Tier 2, Tier 2 to Tier 1 etc.

International Trade

The IA includes a section that comments on the potential trade impacts, where it notes that the regulations could affect inward investment flows, in particular where global providers are required to alter processes or move functionality to the UK.

The IA briefly mentions that inward investment will be key, but the IA would benefit from further discussion on whether the introduction of the 5G and full fibre networks

are dependent upon investment from international firms, and as a result of this new legislation, might face further barriers to the rollout of these networks.

Distributional

An equalities impact assessment has been undertaken, with the IA including some of the findings related to the current limited usage of 5G networks, as well as figures on households that are digitally excluded. The IA would benefit from the inclusion of discussion on the regional and rural-urban variations in the quality of existing network/service provision and the rate that it will be rolled out to these areas, as well as the reliance on these networks by local, often small, businesses.

Other

The Department discuss the potential for costs to be passed through by providers and onto consumers. The IA would be improved if the Department were able to express this as a potential percentage increase in bills or prices faced by consumers.

Monitoring and evaluation plan

The Department commits to undertaking a post-implementation review (PIR) for the security framework by 2027, while also proposing to review the Code of Practice on a regular basis. The IA includes a provisional, yet detailed, PIR plan to be administered by Ofcom. In the plan the Department, for a range of key objectives, identify what data will be collated and how this will be used to evaluate the achievement of the policy objectives.

The IA discusses how rapid changes in technology and innovation more generally, pose challenges for the monitoring of the regulations. As such, the Department commit to updating the M&E activities to support the PIR to reflect any emerging issues accordingly. The Department note the fast-moving nature of this policy and they commit to include some form of ongoing monitoring and review process, to address the uncertainty of the evidence base.

The IA includes discussion of how the current regulatory system is monitored, citing the work that Ofcom currently does to monitor business compliance. It also discusses the current statutory obligation of providers to report any security breaches to Ofcom. While the IA states that information produced and collated by Ofcom will be used to help Government decide if the Code of Practice and the regulations are still fit-for-purpose, it does not set out how this will be determined.

Regulatory Policy Committee

For further information, please contact regulatoryenquiries@rpc.gov.uk. Follow us on Twitter @RPC_Gov_UK, LinkedIn or consult our website www.gov.uk/rpc. To keep informed and hear our views on live regulatory issues, subscribe to our blog.