Telecoms security: proposal for new regulations and draft code of practice: ISPA Response

About ISPA

ISPA is the trade association for providers of internet services in the UK. We have approximately 150 members, 90% of which are SMEs, as well as large multinational companies. Our members provide internet access, hosting and a wide range of other services to consumers and businesses and we represent a wide eco-system of providers including those that build their own networks and those that resell services via fixed and wireless networks.

Introduction

ISPA welcomes the opportunity to respond to this consultation. We have been following the progress of this policy for several years, helping members understand the new security framework and representing their views to government and parliamentarians. This is both for the industry as a whole but lower tier companies in particular. We are broadly supportive of the aims of the proposals, and welcome government leadership as threats evolve.

That said, the new framework is a notable strengthening of regulations and standards. It marks a new departure through a prescriptive, interventionist regime combined with ambitious implementation deadlines and large enforcement penalties. In summary, our response calls for:

- A less prescriptive approach that gives members more flexibility to meet the aims and outcomes of the regulations
- Changes to the tiering system so that it better meets its proportionality aims, does not act as a disincentive to innovation or barrier to market entry and provides industry with clarity
- More time for all providers to implement the 125+ requirements, bringing Tier 1 deadlines in line with Tier 2, while giving Tier 2 more flexibility and time
- Particular help and guidance with cascading the requirements through the supply chain
- Ongoing engagement between industry, government and regulators to ensure the framework is clear and workable

The new framework is described by government as 'unprecedented' and coincides with powers to limit the use of High Risk Vendors. Coming at a time of great change in the sector, and as supply chains are disrupted, we urge in the strongest possible terms not to rush implementation of the measures. Security policy is often characterised as a balance between security and innovation, as drafted the new requirements tip too strongly towards security. By listening to our and industry's concerns, innovation and investment can continue to flourish while strengthening security.

Impact of the regulations and code of practice on providers

Q1. Do you agree that the requirements set out in the draft regulations and the guidance measures set out in the draft code of practice are an appropriate and proportionate response to address the risks of a security compromise to public telecoms networks and services under the new duties (s.105A and 105C) in the Act? If no please set out why, specifically referencing the particular risk of a security compromise, requirements in the draft regulations, guidance measures in the draft code of practice, and objectives of each section.

The draft regulations and code consist of a significant set of new prescriptive requirements with ambitious timelines for implementation. Generally, there seems to be a mismatch between the

requirements in the draft regulations and the very detailed requirements set out in the draft code. To help with this, we feel it would be more appropriate and proportionate to take a less prescriptive approach in meeting the obligations. An outcome-based approach would allow greater flexibility and room for industry to demonstrate compliance in more than a single way.

The prescriptive granular approach raises concerns over duplication, and we would urge more flexibility than the draft code affords. Security is a priority for our members with policies and practices in place to manage security and mitigate compromises, ensure quality of service and protect customers and ultimately their reputation. Existing policies and practices may already meet or exceed the regulations and we are concerned that this could be undermined or discarded to fit with the draft code. We would welcome assurances from government that there can be a greater degree of flexibility where existing policies and practices meet the same outcomes.

Specifically on points in the draft regulations and code, we would like to raise concerns with the following areas.

Supply chains and renegotiating contracts

Some of the most significant and challenging requirements are contained in Regulation 7 and the draft Code measures that require changes to supply chains. The obligations are placed only on one part of the telecoms supply chain – the provider of a network or service – rather than across the sector. Government should engage more with the whole supply chain in considering how best to cascade the obligations in a more proportionate and targeted manner. This is particularly apt as government intervenes and disrupts the telecoms vendor market, encouraging new entrants and providing funding through the new Telecoms Lab and ORAN investment.

The requirements will be met primarily through renegotiating contracts with suppliers. Telecoms supply chains are large and complex, often defined by interlinked networks and services at various levels, and companies of varying size and scale, and subject to regular M&A activity. We are particularly concerned about the practicalities of having to agree new contracts with multinational suppliers, including suppliers significantly larger than our members. The short timeframes for implementation only add to our concerns. DCMS should not underestimate the scale of the challenge. We ask government to assist through a collective approach, for example providing model contracts to take out to the supply chain. This would go some way to addressing our concerns.

We understand that the obligations are being placed on providers to force them to push through the supply chain. However, we question what happens if parts of the supply chain are unable to meet the requirements either against the draft code's deadlines or even at all? If this then requires providers to procure from different suppliers in a market where there is only a finite number, it adds another level of complexity. Additionally, since government policy on telecoms supply chains shifted in recent years, pressures on global supply chains have magnified for multiple reasons outside of a UK provider's control. This situation suggests more time should be given to implement the measures.

Finally, as the code changes over time, it is important that this happens in consultation with providers and suppliers. Where changes affect providers' supply chains it makes sense to include the parts of the supply chain likely to be impacted. We would welcome an ongoing forum and dialogue between industry and government to oversee this in a transparent manner.

Localisation

The draft regulations include specific measures to minimise the reliance on overseas services and the promotion of data localisation. We welcome improvements to the revised draft regulations that have

clarified this to prohibit services located or accessed from particular countries rather than a blanket prohibition. However, the obligation to maintain a UK service as a fallback option 'without reliance on overseas persons, equipment or stored data' remains. We would welcome further clarity in what instances this will be required. Specifically, points 23.06 and 23.07 in the draft code contains a specific requirement to operate services for one month without relying on international connections if the need arises. This is ranked in the most onerous of requirements and part of the final third wave. In keeping with our main argument to give members more time and take a less prescriptive approach, we question why a one-month period in particular is required.

Ultimately, Regulation 3 still requires limits to off-shoring of services and data. It is arguable how much of a softening this represents and could pose a challenge for all providers, particularly those that operate internationally and in a world of cloud services and SaaS. The increasing push for localisation represents a big departure in policy, it is important that government does not underestimate the challenge, and sufficient time is allowed to plan and prepare for this, with help guidance provided by government.

Impact on resellers

A sizeable part of the UK telecoms market is based around providers reselling infrastructure and services from wholesalers. Resellers do not own any part of their network and are resellers of communication services, yet some will be categorised as Tier 1 (or Tier 2) and this will create situations in which both wholesalers (Company A) and resellers (Company B) are classed within the same tiers. While the regulations draw a distinction between providers of communications networks and services, we are concerned that this does reflect this fully.

Ofcom intends to take a supervisory role of providers' ongoing compliance journey using information gathering powers (S.135) every 6-9 months to establish and analyse adherence to the Code and regulations. Ofcom's proposal does not specifically reference their expectation for resellers within the Tiering structure and information provisions. As such, we are concerned that Ofcom will be requesting information from Company B who would be reliant on Company A for the provision of the specified network information. We believe a more efficient and pragmatic approach would be to identify the resellers and network providers when Ofcom confirm the tier levels of each provider and request the relevant information from the network providers rather than the resellers. This avoids any duplication therefore creating efficiencies and also allows for a timelier response to the information request.

CPE replacement

Another aspect of the UK market is a specific B2B market that provides business grade services. Business customers often receive more dedicated services with SLAs that come at a premium – in fact cybersecurity is often provided as a service to business customers with specific CPE provision and requirements as part of the contract. Due to the customised nature and often specialised knowledge of the customer, business grade connectivity is traditionally subject to less regulation than standard consumer service. We therefore feel that more granularity needs to be provided where the generic TSA requirements are less applicable to business services. To give an example, we believe, CPE replacement (11.02) is not appropriate for large business customers where CPE is subject to contracting rules and service level agreements defined in the contract. Unsolicited replacements with no cost to the customer would be a disproportionate response.

Virtualisation

The virtualisation requirements (Section 14) contains measures that members have highlighted run contrary to modern virtualisation design, namely:

- The use of separate physical ports to segregate internal and external networks
- Functions supporting the administration and security not being run on the fabric it is administrating does not align to VMware recommended practice.

Q2. Do you agree it is sufficiently clear which guidance measures in the draft code of practice relate to which regulation (or regulations) within the draft regulations? If no please explain why.

The Code of Practice is a thorough document that provides a great deal of detail and background information on the regulations. However, the scale of the measures demanded of industry means it can be quite a hard document to follow, with examples of different rules in the code to meet a particular regulation not always aligning with the same implementation deadlines.

Q3. Do you expect the draft regulations and draft code of practice to have cost impacts on your business? If yes, please respond to the separate cost survey.

N/A

Tiering

We have grouped are responses to the tiering questions into one section to help provide a clear response.

Q4. Do you agree that differences between public telecoms providers should be recognised within the code of practice via a system of tiering? If no, please explain the reasons for your answer.

Q5. Do you agree that relevant turnover should be used as the metric for determining which tier applies to a given provider? If not, are there other metrics that should be used as an alternative or in combination?

Q6. If YES to question 5 above, do you agree that the existing definition of relevant turnover should be adopted for the purpose of the code of practice?

Q7. Do you agree that the thresholds for each tier should be as below? If no, what alternatives would be most appropriate?

Q8. If you would be impacted by the proposed tiers, would the tier within which you are placed impact the costs of implementing the requirements?

Q9. If you would fall into Tier 3 under the proposals, do you consider it is sufficiently clear how the draft code of practice applies to you and how you would implement relevant guidance measures? If not, would you want additional guidance and if so, on what aspects of the draft regulations?

Q10. Do you agree with the proposed approach to preventing excessive fluctuation between tiers, with a tier designation applying if a provider meets either of the following criteria? If no, what alternatives would be most appropriate and why?

We agree that differences between service providers should be recognised through a tiering system. ISPA has consistently called for a proportionate approach to the new framework to recognise the breadth and complexity of industry, as well the level of resource and customer base. There are more than hundreds if not thousands of communications service providers and the sector is undergoing

significant change, with an array of new market entrants upgrading the UK's fixed broadband. It is only right that a tiered approach should reflect the current market with flexibility as things evolve.

On the face of it, the approach set out in the code of practice of three distinct tiers based on relevant turnover is a sensible, practical and transparent design. However, our industry is complex and we are concerned that this approach fails to address this complexity. Moreover, the approach could be completely undermined by a new addition in the consultation that will require lower tier providers to comply with a higher tier where they provide services to them.

Unintended consequences

As drafted the proposed tiers risk unintended consequences.

The broadband sector has grown and matured in recent years, with scores of new providers building networks locally, regionally and nationally. There are further developments in the market that make this particularly pertinent: significant movement in the market with an increase in M&A activity and a clear expectation of consolidation; and an increase in providers that either offer or take part in the wholesale market. In both cases, we can expect that Tier 3 (and to certain degree Tier 2) providers will need to over-comply right from the get-go, effectively threatening the whole idea of a proportionate system. Only providers that do not expect to grow or take part in the wholesale market will benefit from the proportionate approach which in our mind creates real barriers to business and is anti-competitive.

The sector is approaching a point of maturity where sizable M&A activity is expected as larger companies buy specialist or smaller providers or smaller providers combine. We are concerned that the framework will penalise this M&A activity. For example, if a Tier 3 provider was bought by a Tier 1, the former would have to immediately work towards a high level of compliance in less than 10 months as things stands. Additionally, if two Tier 3 providers with a combined turnover of more than £60m merged, they would both be expected to move towards Tier 2 compliance very quickly. As stated, the likelihood of these scenarios being realised is set to grow markedly as the industry undergoes a period of consolidation.

The approach will also make it more difficult for smaller providers to bid for Government contracts under the Project Gigabit programme. The current terms to bid for funding already includes a high barrier for entry, the suggested approach to the tiering system will only raise this higher as under the contracts providers are required to offer passive infrastructure and wholesale access. In practice, therefore, all smaller providers that win Project Gigabit contracts will need to be Tier 1 compliant immediately. This cannot be government's intention.

Finally, resellers are still required to comply with all requirements from their tier, despite some of the information already being submitted by their wholesalers. This duplication is both unnecessary and confusing, we would urge government to minimise the potential for compliance duplication and reporting.

Tier levels

We support a proportionate tiered approach that recognises the difference between providers.

- **Tier 3**: We agree with a lower third tier where companies are only subject to the requirements in the code and active Ofcom monitoring when they reach a certain threshold and £50m feels a sensible figure. We do not agree that moving providers in a lower tier up a tier is an effective way to manage situations where they provide a service to a higher tier as

it undermines the point of a tiered system. It would be overly complex, the definition of services or data in scope is too broad, and defeats the point where smaller operators get more time to implement given less resources. We recommend this requirement is removed.

- **Tier 2**: The band for tier 2 is drawn widely and as drafted would capture a broad array of providers who would be expected to achieve a significant level of compliance, albeit with two additional years to do so. As set out earlier, the broadband market is undergoing significant change, with dozens of companies working towards ambitious growth targets that could see many more providers moving into Tier 2 quite early on in the life of the new regime. The addition of an interim tier to manage growth in the market is welcome but does not go far enough to address this. Tier 2 providers should be given adequate support and timing for implementation.

- **Tier 3:** We understand the rationale for a highest Tier aimed at the largest providers. The proposed approach however lacks proportionality. Tier 1 providers have large and complex networks and are more likely to be impacted by the High Risk Vendor directions and an overall pressures on resource.

Taking all of the above into account, and given the sheer volume of requirements set out for top two tiers and the added uncertainty of Tier 3 providers being brought into scope by stealth, we urge government to allow more time for implementation of the framework. With the first deadline less than ten months away and the final requirements and regulations still being consulted upon, the proposed timings should be reviewed.

We therefore call on government to:

- Align the Tier 1 deadlines to Tier 2, giving Tier 1 an extra two years to comply
- Give Tier 2 providers greater flexibility and more time to meet the deadlines
- Confirm that Tier 3 providers would not be expected to comply with requirements of higher tiers. If this is not possible, only in exceptional circumstances should this be required.

Tier fluctuation

We agree with an interim tier to prevent excessive fluctuation and provide clarity to industry. This is particularly important in light of the innovation and growth we are seeing in the broadband sector. However, when moving up a tier, members would be keen to understand how much time would be given to implement the measures associated with the relevant tier. So if for example a Tier 3 moves up to Tier 2 in 2024, would they be given more time to meet the requirements than providers designated Tier 2 from the outset?

To address this, we recommend the fluctuation should be clarified so that the 2-year transition period is extended to all examples of fluctuations and not just the two circumstances set out in the consultation.

Turnover

Provided our concerns about proportionality are addressed, we agree that relevant turnover is the most appropriate metric for determining the tier levels. It is clear, transparent and gives a generally good picture of the size and scale of a provider. ISPA members are looking for certainty and to plan for future regulatory changes, and the turnover metric provides this to a large extent. As the new framework is embedded and over time, we could see value in looking again at whether a risk-based approach could be a more effective measure than turnover, but at this stage turnover makes sense.

We would welcome further clarity on exactly what 'relevant turnover' is defined as. If for example, a telecoms provider offers a range of services beyond connectivity (for example hosting or a managed service) would this form part of relevant turnover?

Impact

As an association, we are not in a position to provide specific detail on the cost impact of the requirements. Anecdotally, member feedback is that it will incur costs in meeting the new requirements, both financial and resource. We have encouraged members to engage with the cost consultation, though are aware that the lack of coordination between this consultation and the cost survey that may impact on the level of response.

As well as the costs of implementation there is also the opportunity cost and time spent meeting the prescriptive requirements. Members already have existing security policies and measures in place, with an approach appropriate to their business and customer base. The new framework will for some involve duplicating or amending existing policies to meet the government's prescriptive requirements. This opportunity and time impact should also be noted, and where existing policies and practices meet the same outcome at the regulations and code should be sufficient.

Legacy networks

Q15. Do you agree that a blanket approach to exempting specific equipment systems as 'legacy networks' is not appropriate given the variation between networks? If no, please explain the reasons for your answer.

Q16. Do you agree that implementation timetables for actions in the draft code of practice should align with existing change programmes such as the planned PSTN switch-off? If no, please explain the reasons for your answer.

Q17. Do you agree with the proposals in the draft regulations and draft code of practice to address risks arising from legacy systems and equipment (such as Regulation 3(1)(b), guidance in section 2 of the draft code of practice and guidance measures including 5.07, 10.14 and 11.05)? If no, please explain the reasons for your answer.

We feel the requirements should make a distinction between specific legacy systems where possible. The sector is undergoing significant change with the PSTN being retired in 2025, at the same time as new full fibre networks are deployed. While we understand the need for consistency to reduce security compromises, expectations should take account of legacy equipment being replaced or retired through a proportionate approach that balances the level of work required against the level of risk posed.

Yes, as stated above members are facing big changes to the sector in the next few years. It is only right that these measures adhere to this and make allowances for any changes. We also feel that there is little benefit to enforce significant change programmes for infrastructure that will be retired soon after anyway and that a more tailored approach would be proportionate to manage risk on legacy systems.