Response to Ofcom consultation:

General policy on ensuring compliance with security duties

Prepared for

INCA

May 2022

GOS Consulting Limited - The Laithe House, Woods Lane, Cliddesden, RG25 2JF, Hampshire, UK

1 Introduction

INCA is a trade association. Its members are supporting, planning, building and operating sustainable, independent and interconnected full fibre and wireless networks that advance the economic and social development of the communities they serve and permit the provision of applications and services through open competition, innovation and diversity.

INCA's aims are to:

- To support the development of the competitive digital infrastructure sector through collaborative activities
- To facilitate networking and knowledge sharing between members, other organisations and public bodies
- To encourage and facilitate joint projects between members that can benefit the sector as a whole
- To represent the interests of members to government, Ofcom and other bodies
- To support the development and adoption of common standards by INCA members to deliver the highest possible quality of services
- To promote the advantages of competitive digital infrastructure provision and consumer choice
- To promote the need for increased labour and skills capacity in the sector

INCA has more than 150 members, including: network owners, operators, and managers; access and middle mile networks; public sector organisations actively promoting the development of 21st century digital infrastructure; vendors, equipment suppliers, and providers of services that support the sector.

2 Executive Summary

Whilst welcoming Ofcom's general supportive approach to monitoring and enforcement of the new TSA, its regulations, and the associated Code of Practice (CoP), INCA notices that Ofcom's entire focus is on Tier 1 and 2 providers, with no mention of support for or dialogue with Tier 3 providers.

Tier 3 providers are subject to the TSA obligations and its regulations just like Tier 1 and 2 providers, but not to the CoP. In reality, this makes compliance with the TSA very complex for Tier 3 providers as no interpretation of what is required has been provided by either Government or Ofcom. This means that the group of providers with the least resources to interpret the TSA and the regulations are left with no support at all, whilst large well-resourced providers benefit from the clarity of the CoP and the ongoing support from Ofcom.

INCA understands that the intention behind the tiering system was likely that efforts should be focused where the highest risk of harm from security breaches exists – and that is from larger providers, but as larger providers increasingly use wholesale access from smaller providers and all/most networks are directly or indirectly interconnected in order to facilitate the 'any to any' principle, there are significant parts of the CoP that flow through to smaller providers – but with no support for how they might achieve compliance and what constitutes compliance.

The purpose of addressing the CoP at Tier 1 and 2 providers was also likely motivated by ensuring that the compliance burden be proportionate to the size and resources of the providers. INCA understands and appreciates that principle, but we fear that the complete vacuum of interpretational guidance to Tier 3 providers increases uncertainty for those providers and risks higher levels of non-compliance. Tier 3 providers do not wish to be considered 'soft spots' for the overall telecommunications network infrastructure in the UK. Guidance on proportionate interpretation of the TSA and its regulations would help prevent that from happening.

With regards to Ofcom's proposals for resilience monitoring, INCA considers that they generally rest in reasonable and proportionate principles, although it would be beneficial for Ofcom to engage with all providers on an ongoing basis with regards to the interpretation of those very high level and general provisions. INCA is particularly concerned, however, by the provision that appears to require providers to inform consumers of the provider's network resilience. INCA does not understand how this could or should be implemented and considers it unduly complex and disproportionate.

3 Introduction

INCA is pleased to respond to Ofcom's consultation on its role as the body responsible for monitoring and enforcing compliance with the measures of the Telecoms Security Act (TSA) and the CoP on which the Government recently concluded its consultation period.

Overall, INCA considers that Ofcom's approach of working collaboratively with providers is the right approach to achieve the best possible compliance with these new and far-reaching measures and obligations on providers.

INCA is, however concerned that Ofcom's consultation addresses only how it will work with Tier 1 and 2 providers, with only a brief mention of Tier 3 providers stating that Ofcom will not proactively engage with this very large group of providers, but will still use its enforcement powers should a Tier 3 provider be found to not comply with its legal obligations.[1]

[1] Paragraph 3.13.

Although, the Code of Practice does not apply directly to Tier 3 providers, the overarching duties under the act do apply.[2] Yet Ofcom offers no assistance with compliance to these many much smaller providers.

INCA and its members urge Ofcom to engage proactively with Tier 3 providers. Whilst they may not be under the same level of pre-specified and time-defined compliance requirements, they nevertheless have to comply with the provisions of the Act. Additionally, if a Tier 3 provider offers interconnection and/or wholesale to a Tier 1 or 2 provider, a large subset of the Code of Practice is applicable to the Tier 3 provider. This is not recognised in Ofcom's approach which offers no support for or dialogue with Tier 3 providers.

4 Ofcom's proposed approach

INCA agrees with Ofcom's proposed overall approach to monitoring and enforcement of compliance by Tier 1 and 2 providers of the TSA and the CoP. We believe that a collaborative and supportive approach is appropriate for what is likely to be very significant programmes of work to change design, equipment, processes, and systems throughout large and complex businesses. Likewise, INCA agrees with Ofcom's approach to testing and reporting for those providers.

INCA's concern is that Ofcom has chosen to provide no transparency of how it proposes to assess compliance by Tier 3 providers. Although the CoP does not apply directly to Tier 3 providers, the provisions of the TSA do. Whilst the Tiering system has no doubt been designed to ease the compliance burden for Tier 3 providers, this will focus efforts on ensuring compliance by large providers with >£50m relevant turnover as security failures in those large providers would affect many more consumers and users of telecommunications

[2] Paragraph 3.8.

services. Nevertheless the legal obligation to comply still exists for the smaller providers and they have been offered no guidance as to what would constitute compliance. As they are not covered by the CoP, we assume that compliance for Tier 3 providers is something different from compliance with the CoP.

Further, large sections of the CoP will apply to Tier 3 providers, if they provide interconnection or access to a higher tier provider. As many or most small network providers need to offer wholesale access in order to have long term viable business models and the Government funding programmes such as Project Gigabit make wholesale access mandatory to any beneficiaries, it is very likely that Tier 3 providers will indeed have to comply with at least parts of the CoP in similar timeframes to Tier 1 and 2 providers. INCA therefore strongly disagrees with Ofcom's proposal to effectively offer no support to Tier 3 providers.

4.1 Wholesale access

The TSA Regulations 7 states as follows:

"7.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.

(2) In this Regulation, "third party supplier", in relation to a network provider or service provider, means a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(3) The risks referred to in paragraph (1) include—

(a)those arising during the formation, existence or termination of contracts with third party suppliers, and

(b)those arising from third party suppliers with whom the network provider or service provider has a contractual relationship contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.

(4)A network provider or service provider ("the primary provider") must take such measures as are appropriate and proportionate—

(a)to ensure, by means of contractual arrangements, that each third party supplier—

(i)takes appropriate measures to identify the risks of security compromises occurring in relation to the primary provider's network or service as a result of the primary provider's use of goods, services or facilities supplied, provided or made available by the third party supplier, to disclose any such risks to the primary provider, and to reduce any such risks,

(ii)where the third party supplier is itself a network provider and is given access to the primary provider's network or service or to sensitive data, take measures for the purposes mentioned in section 105A(1) of the Act equivalent to those that the primary provider is required to take in relation to the primary provider's network or service,

(iii)takes appropriate measures to enable the primary provider to monitor all activity undertaken or arranged by the third party supplier in relation to the primary provider's network or service, and

(iv)takes appropriate measures to co-operate with the primary provider in the resolution of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary provider's network or service or of an increased risk of such a compromise occurring,

(b)to ensure that all network connections and data sharing with third party suppliers, or arranged by third party suppliers, are managed securely, and

(c)to have appropriate written plans to manage the termination of, and transition from, contracts with third party suppliers while maintaining the security of the network or service."

When tracking through the CoP, a large number of provisions cross reference Regulation 7 and, whilst indirectly through contractual provisions rather than directly as a subject to the CoP, any Tier 3 provider offering wholesale access would, at a minimum, be required to comply with those provisions. This means that as soon as the Tier 1 and 2 providers have to comply, the Tier 3 providers providing access also have to do so, and yet Ofcom offers no support at all for this large group of providers.

With regards to Interconnection, all small providers that offer a voice service will somehow interface with large providers. Some small providers use third parties to manage their voice service offerings, but this does not mean that their networks do not interact with at least one large provider (or they are a sub-provider to a party that does) and the requirements will be back-to-back in order to cover the Tier 1 and 2 provider CoP compliance requirements.

4.2 Unintended consequences of the tiering system

We attach to this response our response to the Government's recent consultation on the CoP. You will see from that, that there clearly are significant risks of significant unintended consequences of the tiering system in the CoP. It would seem to us that the tiering system will in many ways work to the direct detriment to small providers, simply because they have been excluded from the Government's (and now Ofcom's) detailed analysis and proposals.

In the attached response, we set out proposals for how Tier 3 providers can be better accommodated in the compliance framework, including providing time for compliance should a Tier 3 provider move into Tier 1 or 2 as a consequence of consolidation. We also propose that, for the purposes of compliance to satisfy wholesale- and interconnection-compliance requirements for Tier 3 providers, a working group should be created to constructively consider how such compliance can be achieved without it becoming an insurmountable barrier for Tier 3 providers that either need to offer interconnection or wholesale services in

order to operate a viable business or who have to offer such services as a condition for receiving state aid. INCA looks to Ofcom to support those requests.

4.3 INCA's proposals

In addition to the proposals set out in the attached response to the Government consultation, INCA proposes the following amendments to Ofcom's proposed approach:

- Ofcom creates a TSA compliance forum for Tier 3 providers (possibly under the auspices of the OTA) in which proportionate compliance options can be developed that are less onerous that those set out in the CoP for Tiers 1 and 2.
- Ofcom facilitates 'Tier 3 compliance surgeries' in which providers can bring to Ofcom specific TSA compliance queries (we recognise that Ofcom cannot offer legal support, this would be at a more practical level and an opportunity for Tier 3 providers to share experiences)
- Ofcom works specifically with providers of all tiers to help create a common understanding of reasonable TSA compliance requirements for wholesale access and interconnection provision to by Tier 3 providers to Tier 1 and 2 providers.

INCA and its members understand the severity of possible security threats to electronic communications networks and services and wish to contribute in the best manner possible towards the minimisation of such threats. The proposal listed above and the issues raised in this response highlight why the current tiering system combined with Ofcom's proposed 'hands-off' approach to Tier 3 operators will make it harder to minimise those threats, not easier.

5 Ofcom's resilience monitoring and enforcement

Overall, INCA considers that Ofcom's proposals are reasonable, although they may be considered very high level, leaving significant discretion for interpretation. This may be necessary and advantageous as technologies, networks and services evolve constantly, but INCA considers that this flexible regime should be accompanied by an approach by Ofcom that is similar to that which it proposes for the monitoring of TSA CoP compliance for Tiers 1 and 2 providers – namely an ongoing dialogue that gives all providers insight into the kind of resiliency measures Ofcom considers reasonable and proportionate and which gives providers an opportunity to work transparently with Ofcom in determining and implementing such measures.

One proposal in particular, however, has raised concerns with INCA's members. This is set out in paragraph 5.23 of Annex 6 to the consultation:

"The risk appetite of end users will vary, so we expect providers to provide information about the resilience of their services to allow customers to make informed purchasing choices. Providers should attempt to match the delivered network and service availability and performance levels to the customer expectations that have been set. More broadly, providers have a duty to inform users about certain risks of security compromise (section 105J). Providers should refer to Section 5 (Reporting security compromises) of the Ofcom Procedural Guidance for further details." [emphasis added]

INCA is not aware of any previous obligations that providers should provide information to customers about the resilience of their services. A number of INCA's members offer service level agreements to all or some of their customers (depending on the services they take), but the need to notify customers in general of their network resilience could require changes to standard terms and conditions or other customer information. Additionally, different parts of network may have different levels of resilience and resilience may change over time. Making too much architecture and network design information public could have the adverse effect

of increasing risk and reducing overall resilience. INCA therefore queries the justification of this provision and seeks clarity as to how Ofcom sees this obligation being applied in practice.